Nessus Report

Nessus Scan Report

09/Jun/2013:14:17:39

HomeFeed: Commercial use of the report is prohibited

Table Of Contents

Hosts Summary (Executive)

iosr_client.cloudfoundry.com

Summary

Critical	High	Medium	Low	Info	Total
0	0	3	2	41	46

Details

Severity	Plugin Id	Name
Medium (5.0)	10539	DNS Server Recursive Query Cache Poisoning Weakness
Medium (4.3)	48432	Web Application Session Cookies Not Marked HttpOnly
Medium (4.3)	49218	Web Application Session Cookies Not Marked Secure
Low (2.6)	26194	Web Server Uses Plain Text Authentication Forms
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Info	10028	DNS Server BIND version Directive Remote Version Disclosure
Info	10107	HTTP Server Type and Version
Info	10195	HTTP Proxy Open Relay Detection
Info	10287	Traceroute Information
Info	10386	Web Server No 404 Error Code Check
Info	10662	Web mirroring
Info	10863	SSL Certificate Information
Info	11002	DNS Server Detection
Info	11032	Web Server Directory Enumeration
Info	11040	HTTP Reverse Proxy Detection
Info	11149	HTTP login page
Info	11153	Service Detection (HELP Request)
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	18528	SMTP Server Connection Check
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported

Info	33817	CGI Generic Tests Load Estimation (all tests)
Info	35371	DNS Server hostname.bind Map Hostname Disclosure
Info	39463	HTTP Server Cookies Set
Info	39470	CGI Generic Tests Timeout
Info	40773	Web Application Potentially Sensitive CGI Parameter Detection
Info	42057	Web Server Allows Password Auto-Completion
Info	42799	Broken Web Servers
Info	43111	HTTP Methods Allowed (per directory)
Info	44987	HTTP Session Cookies
Info	45590	Common Platform Enumeration (CPE)
Info	46180	Additional DNS Hostnames
Info	47830	CGI Generic Injectable Parameter
Info	47863	Web Tests Session Expiration Errors
Info	49704	External URLs
Info	51891	SSL Session Resume Supported
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	58768	SSL Resume With Different Cipher Issue
Info	62563	SSL Compression Methods Supported
Info	66334	Patch Report

Vulnerabilities By Plugin

48432 (2) - Web Application Session Cookies Not Marked HttpOnly

Synopsis

HTTP session cookies might be vulnerable to cross-site scripting attacks.

Description

The remote web application uses cookies to track authenticated users. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script such as JavaScript could read them.
'HttpOnly' is a security mechanism to protect against cross-site scripting attacks that was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers support it.
Note that :
- 'HttpOnly' can be circumvented in some cases.
- The absence of this attribute does not mean that the web application is automatically vulnerable to cross-site scripting attacks.
- Some web applications need to manipulate the session cookie through client-side scripts and the 'HttpOnly' attribute cannot be set.

See Also

http://www.nessus.org/u?916b20e4

http://www.nessus.org/u?6752aae7

Solution

If possible, add the 'HttpOnly' attribute to all session cookies.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2010/08/25, Modification date: 2013/01/25

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
The session cookie is not marked 'HttpOnly'.

Here is the insecure cookie :

Name : JSESSIONID
Path : /
Value : 6925B29584C1B026DFB81C8465B29DC9
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

iosr_client.cloudfoundry.com (tcp/443)

```
The session cookie is not marked 'HttpOnly'.

Here is the insecure cookie :

Name : JSESSIONID
Path : /
Value : 6925B29584C1B026DFB81C8465B29DC9
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
```

```
Port :
```

49218 (2) - Web Application Session Cookies Not Marked Secure

Synopsis

HTTP session cookies may be sent in clear text.

Description

The remote web application uses cookies to track authenticated users. However, there are instances where the application is running over unencrypted HTTP or the cookie(s) are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances.
As a result, it may be possible for a remote attacker to intercept these cookies.

See Also

http://www.nessus.org/u?916b20e4

Solution

- Host the web application on a server that only provides SSL (HTTPS).
- Mark all cookies as 'secure'.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

XREF	CWE:522
XREF	CWE:718
XREF	CWE:724

Plugin Information:

Publication date: 2010/09/14, Modification date: 2013/01/25

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
The web application is available via
insecure HTTP.
```

iosr_client.cloudfoundry.com (tcp/443)

```
The session cookie is not marked 'secure'.

Here is the insecure cookie :

Name : JSESSIONID
Path : /
Value : 6925B29584C1B026DFB81C8465B29DC9
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

10539 (1) - DNS Server Recursive Query Cache Poisoning Weakness

Synopsis

The remote name server allows recursive queries to be performed by the host running nessusd.

Description

It is possible to query the remote name server for third party names.
If this is your internal nameserver, then the attack vector may be limited to employees or guest access if allowed.
If you are probing a remote nameserver, then it allows anyone to use it to resolve third party names (such as www.nessus.org).
This allows attackers to perform cache poisoning attacks against this nameserver.
If the host allows these recursive queries via UDP, then the host can be used to 'bounce' Denial of Service attacks against another network or system.

See Also

http://www.nessus.org/u?c4dcf24a

Solution

Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it).
If you are using bind 8, you can do this by using the instruction 'allow-recursion' in the 'options' section of your named.conf.
If you are using bind 9, you can define a grouping of internal addresses using the 'acl' command.
Then, within the options block, you can explicitly state:
'allow-recursion { hosts_defined_in_acl }'
If you are using another name server, consult its documentation.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

4.3 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

References

BID	136
BID	678
CVE	CVE-1999-0024
XREF	OSVDB:438
XREF	CERT-CC:CA-1997-22

Plugin Information:

Publication date: 2000/10/27, Modification date: 2012/12/10

Hosts

iosr_client.cloudfoundry.com (udp/53)

26194 (1) - Web Server Uses Plain Text Authentication Forms

Synopsis

The remote web server might transmit credentials in cleartext.

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.
An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:718
XREF	CWE:724

Plugin Information:

Publication date: 2007/09/28, Modification date: 2011/09/15

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
Page : /administrator/edit/9
Destination page : /administrator/edit/9
Input name : password
Default value :  123


Page : /administrator/edit/11
Destination page : /administrator/edit/11
Input name : password
Default value :  123


Page : /administrator/add
Destination page : /administrator/add
Input name : password


Page : /administrator/edit/9?
id=9&login=ala&password=123&email=ala@example.com&name=Ala&surname=Nowak&tenantName=AGH&enabled=true&commit=Up
Destination page : /administrator/edit/9
Input name : password
Default value :  123


Page : /administrator/edit/11?
id=11&login=marcin&password=123&email=marcin@example.com&name=Marcin&surname=Wrog&tenantName=AGH&enabled=false
Destination page : /administrator/edit/11
Input name : password
Default value :  123


Page : /administrator/add?id=&login=&password=&email=&name=&surname=&tenantName=UJ&commit=Add
Destination page : /administrator/add
Input name : password
```

```
Page : /administrator/edit/9?
id=9&login=ala&password=123&email=ala@example.com&name=Ala&surname=Nowak&tenantName=AGH&enabled=false&commit=U
Destination page : /administrator/edit/9
Input name : password
Default value :  123


Page : /administrator/edit/11?
id=11&login=marcin&password=123&email=marcin@example.com&name=Marcin&surname=Wrog&tenantName=AGH&enabled=true&
Destination page : /administrator/edit/11
Input name : password
Default value :  123


Page : /administrator/edit/9?
id=9&login=ala&password=123&email=ala@example.com&name=Ala&surname=Nowak&tenantName=PK&enabled=true&commit=Upd
Destination page : /administrator/edit/9
Input name : password
Default value :  123


Page : /administrator/edit/11?
id=11&login=marcin&password=123&email=marcin@example.com&name=Marcin&surname=Wrog&tenantName=PK&enabled=false&
Destination page : /administrator/edit/11
Input name : password
Default value :  123
```

65821 (1) - SSL RC4 Cipher Suites Supported

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.
If plaintext is repeatedly encrypted (e.g. HTTP cookies), and an attacker is able to obtain many (i.e. tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

2.2 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

BID	58796
CVE	CVE-2013-2566
XREF	OSVDB:91162

Plugin Information:

Publication date: 2013/04/05, Modification date: 2013/04/05

Hosts

iosr_client.cloudfoundry.com (tcp/443)

```
Here is the list of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=MD5
      RC4-SHA                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=SHA1

    TLSv1
      RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=MD5
      RC4-SHA                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

11219 (4) - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Hosts

iosr_client.cloudfoundry.com (tcp/25)

```
Port 25/tcp was found to be open
```

iosr_client.cloudfoundry.com (tcp/80)

```
Port 80/tcp was found to be open
```

iosr_client.cloudfoundry.com (tcp/443)

```
Port 443/tcp was found to be open
```

iosr_client.cloudfoundry.com (tcp/3128)

```
Port 3128/tcp was found to be open
```

22964 (4) - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/05/12

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
A web server is running on this port.
```

iosr_client.cloudfoundry.com (tcp/80)

```
An HTTP proxy is running on this port.
```

iosr_client.cloudfoundry.com (tcp/443)

```
A TLSv1 server answered on this port.
```

iosr_client.cloudfoundry.com (tcp/443)

```
A web server is running on this port through TLSv1.
```

10662 (3) - Web mirroring

Synopsis

Nessus crawled the remote web site.

Description

This script makes a mirror of the remote web site(s) and extracts the list of CGIs that are used by the remote host.
It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/05/04, Modification date: 2013/04/11

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/tenant/edit/6 (id [6] name [UJ] enabled [true] commit [Update] description [Uniwersyt...)
/administrator/remove (itemIds [9] itemIds [11] )
/administrator/edit/11 (enabled [false] id [11] surname [Wrog] password [123] commit [Update] ...)
/stockQuote/list ()
/tenant/add (name [] commit [Add] description [] )
/stockCompanies/remove (symbols [GOOG] symbols [NVDA] )
/tenant/edit/7 (id [7] name [PK] enabled [true] commit [Update] description [Politechn...)
/stockCompanies/update (symbol [] name [] commit [OK] )
/administrator/add (id [] name [] surname [] login [] email [] tenantName [UJ] commit [Add...)
/tenant/edit/5 (id [5] name [AGH] enabled [false] commit [Update] description [Akademi...)
/administrator/edit/9 (enabled [true] id [9] surname [Nowak] password [123] commit [Update] e...)
/tenant/edit/4 (id [4] name [SUPERUSER_TENANT] enabled [true] commit [Update] descript...)
/tenant/remove (itemIds [4] itemIds [5] itemIds [6] itemIds [7] )

60 requests were sent in 20.929 s = 2 req/s = 348 ms/req
```

iosr_client.cloudfoundry.com (tcp/443)

```
The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/tenant/edit/6 (id [6] name [UJ] description [Uniwersytet Jagiellonski] enabled [false...)
/administrator/remove (itemIds [9] itemIds [11] )
/administrator/edit/11 (enabled [false] id [11] surname [Wrog] password [123] commit [Update] ...)
/stockQuote/list ()
/tenant/add (name [] commit [Add] description [] )
/stockCompanies/remove (symbols [GOOG] symbols [NVDA] )
/tenant/edit/7 (id [7] name [PK] description [Politechnika Krakowska] enabled [false] ...)
/stockCompanies/update (symbol [] name [] commit [OK] )
/administrator/add (id [] name [] surname [] login [] email [] tenantName [UJ] commit [Add...)
/tenant/edit/5 (id [5] name [AGH] description [Akademia Gorniczo-Hutnicza] enabled [tr...)
/j_spring_security_check (j_username [] j_password [] commit [Log in] )
/administrator/edit/9 (enabled [true] id [9] surname [Nowak] password [123] commit [Update] e...)
/tenant/edit/4 (id [4] name [SUPERUSER_TENANT] enabled [true] commit [Update] descript...)
/tenant/remove (itemIds [4] itemIds [5] itemIds [6] itemIds [7] )

56 requests were sent in 35.273 s = 1 req/s = 629 ms/req
```

iosr_client.cloudfoundry.com (tcp/3128)

```
1 requests were sent in 7.012 s = 0 req/s = 7012 ms/req
```

11149 (3) - HTTP login page

Synopsis

HTTP form based authentication.

Description

This script logs onto a web server through a login page and stores the authentication / session cookie.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/10/26, Modification date: 2013/05/14

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
HTTP login succeeded
```

iosr_client.cloudfoundry.com (tcp/443)

```
HTTP login succeeded
```

iosr_client.cloudfoundry.com (tcp/3128)

```
HTTP login failed :
request failed: GET /login
```

39463 (3) - HTTP Server Cookies Set

Synopsis

Some cookies have been set by the web server.

Description

HTTP cookies are pieces of information that are presented by web servers and are sent back by the browser.
As HTTP is a stateless protocol, cookies are a possible mechanism to keep track of sessions.
This plugin displays the list of the HTTP cookies that were set by the web server when it was crawled.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/06/19, Modification date: 2011/03/15

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
This cookie was set by Tomcat(servlet/jsp engine) :
path     = /
name     = JSESSIONID
value    = 6925B29584C1B026DFB81C8465B29DC9
version  = 1
secure   = 0
httponly = 0

path     = /
name     = __VCAP_ID__
value    = be3204a2a4119f0bdcb0cbfa2ccd90b0c67a8585385d310a7956cf624ec377a5
version  = 1
secure   = 0
httponly = 0
```

iosr_client.cloudfoundry.com (tcp/443)

```
This cookie was set by Tomcat(servlet/jsp engine) :
path     = /
name     = JSESSIONID
value    = 6925B29584C1B026DFB81C8465B29DC9
version  = 1
secure   = 0
httponly = 0

path     = /
name     = __VCAP_ID__
value    = be3204a2a4119f0bdcb0cbfa2ccd90b0c67a8585385d310a7956cf624ec377a5
version  = 1
secure   = 0
httponly = 0
```

iosr_client.cloudfoundry.com (tcp/3128)

```
This cookie was set by Tomcat(servlet/jsp engine) :
path     = /
name     = JSESSIONID
value    = 6925B29584C1B026DFB81C8465B29DC9
version  = 1
secure   = 0
httponly = 0

path     = /
name     = __VCAP_ID__
value    = be3204a2a4119f0bdcb0cbfa2ccd90b0c67a8585385d310a7956cf624ec377a5
version  = 1
secure   = 0
httponly = 0
```

10107 (2) - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2013/06/03

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
The remote web server type is :

nginx
```

iosr_client.cloudfoundry.com (tcp/443)

```
The remote web server type is :

nginx
```

10195 (2) - HTTP Proxy Open Relay Detection

Synopsis

The remote web proxy server accepts requests.

Description

The remote web proxy accepts unauthenticated HTTP requests from the Nessus scanner. By routing requests through the affected proxy, a user may be able to gain some degree of anonymity while browsing web sites, which will see requests as originating from the remote host itself rather than the user's host.

Solution

Make sure access to the proxy is limited to valid users / hosts.

Risk Factor

None

Plugin Information:

Publication date: 1999/06/22, Modification date: 2013/01/02

Hosts

iosr_client.cloudfoundry.com (tcp/80)
iosr_client.cloudfoundry.com (tcp/3128)

24260 (2) - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
Protocol version : HTTP/1.0
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Language: en
  Content-Length: 1486
  Content-Type: text/html; UTF-8;charset=UTF-8
  Date: Sun, 09 Jun 2013 12:57:32 GMT
  Server: Apache-Coyote/1.1
  X-Cache: MISS from plus.ds14.agh.edu.pl
  X-Cache-Lookup: MISS from plus.ds14.agh.edu.pl:3128
  Via: 1.0 plus.ds14.agh.edu.pl:3128 (squid)
  Connection: keep-alive
```

iosr_client.cloudfoundry.com (tcp/443)

```
Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Server: nginx
  Date: Sun, 09 Jun 2013 12:57:36 GMT
  Content-Type: text/html; UTF-8;charset=UTF-8
  Content-Length: 1486
  Connection: keep-alive
  Keep-Alive: timeout=20
  Content-Language: en
```

33817 (2) - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.
The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.
Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/10/26, Modification date: 2013/01/29

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

on site request forgery                  : S=9          SP=9         AP=9         SC=9
 AC=9
SQL injection                            : S=1320       SP=4392      AP=4392      SC=23544
 AC=23544
unseen parameters                        : S=1925       SP=6405      AP=6405      SC=34335
 AC=34335
local file inclusion                     : S=55         SP=183       AP=183       SC=981
 AC=981
web code injection                       : S=55         SP=183       AP=183       SC=981
 AC=981
XML injection                            : S=55         SP=183       AP=183       SC=981
 AC=981
format string                            : S=110        SP=366       AP=366       SC=1962
 AC=1962
script injection                         : S=9          SP=9         AP=9         SC=9
 AC=9
cross-site scripting (comprehensive test): S=220        SP=732       AP=732       SC=3924
 AC=3924
injectable parameter                     : S=110        SP=366       AP=366       SC=1962
 AC=1962
cross-site scripting (extended patterns) : S=54         SP=54        AP=54        SC=54
 AC=54
directory traversal (write access)       : S=110        SP=366       AP=366       SC=1962
 AC=1962
SSI injection                            : S=165        SP=549       AP=549       SC=2943
 AC=2943
header injection                         : S=18         SP=18        AP=18        SC=18
 AC=18
directory traversal                      : S=1375       SP=4575      AP=4575      SC=24525
 AC=24525
HTML injection                           : S=45         SP=45        AP=45        SC=45
 AC=45
arbitrary command execution (time based) : S=330        SP=1098      AP=1098      SC=5886
 AC=5886
persistent XSS                          [...]
```

iosr_client.cloudfoundry.com (tcp/443)

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

cross-site scripting (comprehensive test): S=232        SP=760       AP=760       SC=3956
 AC=3956
```

```
persistent XSS                          : S=232       SP=760       AP=760       SC=3956
 AC=3956
arbitrary command execution             : S=928       SP=3040      AP=3040      SC=15824
 AC=15824
web code injection                      : S=58        SP=190       AP=190       SC=989
 AC=989
HTML injection                          : S=15        SP=15        AP=15        SC=15
 AC=15
arbitrary command execution (time based) : S=348      SP=1140      AP=1140      SC=5934
 AC=5934
script injection                        : S=3         SP=3         AP=3         SC=3
 AC=3
XML injection                           : S=58        SP=190       AP=190       SC=989
 AC=989
unseen parameters                       : S=2030      SP=6650      AP=6650      SC=34615
 AC=34615
directory traversal (write access)      : S=116       SP=380       AP=380       SC=1978
 AC=1978
SQL injection (2nd order)               : S=58        SP=190       AP=190       SC=989
 AC=989
on site request forgery                 : S=3         SP=3         AP=3         SC=3
 AC=3
blind SQL injection (4 requests)        : S=232       SP=760       AP=760       SC=3956
 AC=3956
HTTP response splitting                 : S=27        SP=27        AP=27        SC=27
 AC=27
directory traversal (extended test)     : S=2958      SP=9690      AP=9690      SC=50439
 AC=50439
header injection                        : S=6         SP=6         AP=6         SC=6
 AC=6
injectable parameter                    : S=116       SP=380       AP=380       SC=1978
 AC=1978
directory traversal                    [...]
```

39470 (2) - CGI Generic Tests Timeout

Synopsis

Some generic CGI attacks ran out of time.

Description

Some generic CGI tests ran out of time during the scan. The results may be incomplete.

Solution

Run your run scan again with a longer timeout or less ambitious options :
- Combinations of arguments values = 'all combinations' is much slower than 'two pairs' or 'single'.
- Stop at first flaw = 'per port' is quicker.
- In 'some pairs' or 'some combinations' mode, try reducing web_app_tests.tested_values_for_each_parameter in nessusd.conf

Risk Factor

None

Plugin Information:

Publication date: 2009/06/19, Modification date: 2011/03/06

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
The following tests timed out without finding any flaw :
- SQL injection
- arbitrary command execution
```

iosr_client.cloudfoundry.com (tcp/443)

```
The following tests timed out without finding any flaw :
- directory traversal
- arbitrary command execution
- cross-site scripting (comprehensive test)
- SQL injection
- SQL injection (on HTTP headers)
```

40773 (2) - Web Application Potentially Sensitive CGI Parameter Detection

Synopsis

An application was found that may use CGI parameters to control sensitive information.

Description

According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. These parameters should be examined to determine what type of data is controlled and if it poses a security risk.
** This plugin only reports information that may be useful for auditors
** or pen-testers, not a real flaw.

Solution

Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.

Risk Factor

None

Plugin Information:

Publication date: 2009/08/25, Modification date: 2012/08/17

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
Potentially sensitive parameters for CGI /tenant/edit/7 :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /administrator/edit/9 :

id : Potential horizontal or vertical privilege escalation
password : Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack

Potentially sensitive parameters for CGI /administrator/edit/11 :

id : Potential horizontal or vertical privilege escalation
password : Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack

Potentially sensitive parameters for CGI /administrator/add :

password : Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack
id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /tenant/edit/4 :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /tenant/edit/5 :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /tenant/edit/6 :

id : Potential horizontal or vertical privilege escalation
```

iosr_client.cloudfoundry.com (tcp/443)

```
Potentially sensitive parameters for CGI /tenant/edit/7 :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /tenant/edit/6 :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /administrator/edit/9 :
```

```
id : Potential horizontal or vertical privilege escalation
password : Possibly a clear or hashed password, vulnerable to dictionary attack

Potentially sensitive parameters for CGI /administrator/edit/11 :

id : Potential horizontal or vertical privilege escalation
password : Possibly a clear or hashed password, vulnerable to dictionary attack

Potentially sensitive parameters for CGI /administrator/add :

password : Possibly a clear or hashed password, vulnerable to dictionary attack
id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /tenant/edit/4 :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /tenant/edit/5 :

id : Potential horizontal or vertical privilege escalation
```

42057 (2) - Web Server Allows Password Auto-Completion

Synopsis

Auto-complete is not disabled on password fields.

Description

The remote web server contains at least HTML form field containing an input of type 'password' where 'autocomplete' is not set to 'off'.
While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

None

Plugin Information:

Publication date: 2009/10/07, Modification date: 2011/09/28

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
Page : /administrator/edit/9
Destination Page : /administrator/edit/9
Input name : password
Default value :  123



Page : /administrator/edit/11
Destination Page : /administrator/edit/11
Input name : password
Default value :  123



Page : /administrator/add
Destination Page : /administrator/add
Input name : password



Page : /administrator/edit/9?id=9&login=ala&password=123&email=ala@examp
le.com&name=Ala&surname=Nowak&tenantName=AGH&enabled=true&commit=Update
Destination Page : /administrator/edit/9
Input name : password
Default value :  123



Page : /administrator/edit/11?id=11&login=marcin&password=123&email=marc
in@example.com&name=Marcin&surname=Wrog&tenantName=AGH&enabled=false&com
mit=Update
Destination Page : /administrator/edit/11
Input name : password
Default value :  123



Page : /administrator/add?id=&login=&password=&email=&name=&surname=&ten
antName=UJ&commit=Add
Destination Page : /administrator/add
Input name : password
```

```
Page : /administrator/edit/9?id=9&login=ala&password=123&email=ala@examp
le.com&name=Ala&surname=Nowak&tenantName=AGH&enabled=false&commit=Update
Destination Page : /administrator/edit/9
Input name : password
Default value :  123



Page : /administrator/edit/11?id=11&login=marcin&password=123&email=marc
in@example.com&name=Marcin&surname=Wrog&tenantName=AGH&enabled=true&comm
it=Update
Destination Page : /administrator/edit/11
Input name : password
Default value :  123



Page : /administrator/edit/9?id=9&login=ala&password=123&email=ala@examp
le.com&name=Ala&surname=Nowak&tenantName=PK&enabled=true&commit=Update
Destination Page : /administrator/edit/9
Input name : password
Default value :  123



Page : /administrator/edit/11?id=11&login=marcin&password=123&email=marc
in@example.com&name=Marcin&surname=Wrog&tenantName=PK&enabled=false&comm
it=Update
Destination Page : /administrator/edit/11
Input name : password
Default value :  123
```

iosr_client.cloudfoundry.com (tcp/443)

```
Page : /login
Destination Page : j_spring_security_check
Input name : j_password



Page : /administrator/edit/9
Destination Page : /administrator/edit/9
Input name : password
Default value :  123



Page : /administrator/edit/11
Destination Page : /administrator/edit/11
Input name : password
Default value :  123



Page : /administrator/add
Destination Page : /administrator/add
Input name : password



Page : /administrator/edit/9?id=9&login=ala&password=123&email=ala@examp
le.com&name=Ala&surname=Nowak&tenantName=PK&enabled=true&commit=Update
```

```
Destination Page : /administrator/edit/9
Input name : password
Default value :  123



Page : /administrator/edit/11?id=11&login=marcin&password=123&email=marc
in@example.com&name=Marcin&surname=Wrog&tenantName=AGH&enabled=false&com
mit=Update
Destination Page : /administrator/edit/11
Input name : password
Default value :  123



Page : /administrator/add?id=&login=&password=&email=&name=&surname=&ten
antName=UJ&commit=Add
Destination Page : /administrator/add
Input name : password



Page : /administrator/edit/9?id=9&login=ala&password=123&email=ala@examp
le.com&name=Ala&surname=Nowak&tenantName=AGH&enabled=true&commit=Update
Destination Page : /administrator/edit/9
Input name : password
Default value :  123



Page : /administrator/edit/11?id=11&login=marcin&password=123&email=marc
in@example.com&name=Marcin&surname=Wrog&tenantName=UJ&enabled=true&commi
t=Update
Destination Page : /administrator/edit/11
Input name : password
Default value :  123



Page : /administrator/add?id=&login=&password=&email=&name=&surname=&ten
antName=AGH&commit=Add
Destination Page : /administrator/add
Input name : password



Page : /administrator/edit/9?id=9&login=ala&password=123&email=ala@examp
le.com&name=Ala&surname=Nowak&tenantName=AGH&enabled=false&commit=Update
Destination Page : /administrator/edit/9
Input name : password
Default value :  123



Page : /administrator/add?id=&login=&password=&email=&name=&surname=&ten
antName=PK&commit=Add
Destination Page : /administrator/a [...]
```

43111 (2) - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/12/10, Modification date: 2013/05/09

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
Based on the response to an OPTIONS request :

  - HTTP methods  DELETE  HEAD  OPTIONS  POST  PUT  TRACE GET
    are allowed on :

    /
    /administrator
    /administrator/edit
    /resources/css
    /resources/images
    /resources/javascript
    /stockCompanies
    /stockQuote
    /tenant
    /tenant/edit


Based on tests of each method :

  - HTTP methods GET HEAD OPTIONS are allowed on :

    /resources/css
    /resources/images
    /resources/javascript

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /administrator
    /stockCompanies
    /stockQuote
    /tenant

  - HTTP method OPTIONS is allowed on :

    /administrator/edit

  - HTTP methods OPTIONS POST are allowed on :

    /tenant/edit
```

iosr_client.cloudfoundry.com (tcp/443)

```
Based on the response to an OPTIONS request :
```

```
  - HTTP methods  DELETE  HEAD  OPTIONS  POST  PUT  TRACE GET
    are allowed on :

    /
    /administrator
    /resources/css
    /resources/images
    /resources/javascript


Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD
    INDEX LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY
    OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE are allowed on :

    /administrator/edit

  - HTTP methods ACL BCOPY BDELETE BMOVE BPROPFIND BPROPPATCH CHECKIN
    CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD INDEX LABEL LOCK
    MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS ORDERPATCH
    PATCH POLL POST PROPFIND PROPPATCH PUT REPORT RPC_IN_DATA
    RPC_OUT_DATA SEARCH SUBSCRIBE UNCHECKOUT UNLOCK UNSUBSCRIBE
    UPDATE are allowed on :

    /cgi-bin/eboard40/
    /stockCompanies
    /tenant/edit

  - HTTP methods ACL BCOPY BDELETE BMOVE BPROPFIND BPROPPATCH CHECKIN
    CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD INDEX LABEL LOCK
    MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS ORDERPATCH
    PATCH POLL POST PROPFIND PROPPATCH PUT REPORT RPC_IN_DATA
    RPC_OUT_DATA SEARCH SUBSCRIBE UNCHECKOUT UNLOCK UNSUBSCRIBE
    UPDATE VERSION-CONTROL are allowed on :

    /stockQuote
    /tenant

  - HTTP methods ACL BCOPY BDELETE BMOVE BPROPFIND BPROPPATCH CHECKIN
    CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD INDEX LABEL LOCK
    MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS ORDERPATCH
    PATCH POLL POST PROPFIND PROPPATCH PUT REPORT RPC_IN_DATA
    RPC_OUT_DATA SEARCH SUBSCRIBE UNCHECKOUT UNLOCK UNSUBSCRIBE
    UPDATE X-MS-ENUMATTS are allowed on :

    /administrator
    /login

  - HTTP methods GET HEAD OPTIONS are allowed on :

    /resources/css
    /resources/images
    /resources/javascript

  - HTTP m [...]
```

44987 (2) - HTTP Session Cookies

Synopsis

HTTP session cookies used on the remote web server can be identified.

Description

The remote web application uses cookies to track authenticated users. By removing the cookies, one-by-one, and checking a protected page, it is possible to identify these cookies.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/03/04, Modification date: 2012/01/31

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
The following cookies are used to track authenticated users :

Name : JSESSIONID
Path : /
Value : 6925B29584C1B026DFB81C8465B29DC9
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

iosr_client.cloudfoundry.com (tcp/443)

```
The following cookies are used to track authenticated users :

Name : JSESSIONID
Path : /
Value : 6925B29584C1B026DFB81C8465B29DC9
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

47830 (2) - CGI Generic Injectable Parameter

Synopsis

Some CGIs are candidate for extended injection tests.

Description

Nessus was able to to inject innocuous strings into CGI parameters and read them back in the HTTP response.
The affected parameters are candidates for extended injection tests like cross-site scripting attacks.
This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester.

Solution

n/a

Risk Factor

None

References

XREF CWE:86

Plugin Information:

Publication date: 2010/07/26, Modification date: 2013/02/17

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
Using the POST HTTP method, Nessus found that :

+ The following resources may be vulnerable to injectable parameter :

+ The 'description' parameter of the /tenant/add CGI :

/tenant/add [description=unqdrg]

-------- output --------
</td>
<td>
<a class="" href="/tenant/edit/74">unqdrg</a>
</td>
<td>
------------------------

+ The 'name' parameter of the /tenant/edit/7 CGI :

/tenant/edit/7 [name=unqdrg]

-------- output --------
</td>
<td>
<a class="" href="/tenant/edit/74">unqdrg</a>
</td>
<td>
------------------------

+ The 'symbol' parameter of the /stockCompanies/update CGI :

/stockCompanies/update [symbol=unqdrg]

-------- output --------
<tr>
<td class="controlColumn">
<input name="symbols" value = "unqdrg" type="checkbox" class="itemCheckb
ox" id="symbol_unqdrg" />
</td>
<td>
------------------------

+ The 'name' parameter of the /administrator/edit/9 CGI :

/administrator/edit/9 [name=unqdrg]
```

```
-------- output --------
</td>
<td>
<a class="" href="/administrator/edit/9">unqdrg</a>
</td>
<td>
------------------------

+ The 'name' parameter of the /administrator/edit/11 CGI :

/administrator/edit/11 [name=unqdrg]

-------- output --------
</td>
<td>
<a class="" href="/administrator/edit/9">unqdrg</a>
</td>
<td>
------------------------

+ The 'password' parameter of the /administrator/add CGI :

/administrator/add [password=unqdrg]

-------- output --------
</td>
<td>
<a class="" href="/administrator/edit/9">unqdrg</a>
</td>
<td>
------------------------

+ The 'name' parameter of the /tenant/edit/4 CGI :

/tenant/edit/4 [name=unqdrg]

-------- output --------
</td>
<td>
<a class="" href="/tenant/edit/74">unqdrg</a>
</td>
<td>
------------------------

+ The 'name' parameter of the /tenant/edit/5 CGI :

/tenant/edit/5 [name=unqdrg]

-------- output --------
</td>
<td>
<a class="" href="/tenant/edit/74">unqdrg</a>
</td>
<td>
------------------------

+ The 'name' parameter of the /tenant/edit/6 CGI :

/tenant/edit/6 [name=unqdrg]

-------- output --------
</td>
<td>
<a class="" href="/tenant/edit/74">u [...]
```

iosr_client.cloudfoundry.com (tcp/443)

```
Using the POST HTTP method, Nessus found that :

+ The following resources may be vulnerable to injectable parameter :

+ The 'enabled' parameter of the /tenant/edit/7 CGI :

/tenant/edit/7 [enabled=unqdrg]
```

```
-------- output --------
<html><head><title>Apache Tomcat/6.0.35 - Error report</title><sty [...]
[...] n is java.lang.IllegalArgumentException: Invalid boolean value [unqdrg]]
org.springframework.web.servlet.FrameworkServlet.processRequest(Fr [...]
org.springframework.web.servlet.FrameworkServlet.doPost(FrameworkS [...]
------------------------

+ The 'enabled' parameter of the /tenant/edit/6 CGI :

/tenant/edit/6 [enabled=unqdrg]

-------- output --------
<html><head><title>Apache Tomcat/6.0.35 - Error report</title><sty [...]
[...] n is java.lang.IllegalArgumentException: Invalid boolean value [unqdrg]]
org.springframework.web.servlet.FrameworkServlet.processRequest(Fr [...]
org.springframework.web.servlet.FrameworkServlet.doPost(FrameworkS [...]
------------------------

+ The 'symbol' parameter of the /stockCompanies/update CGI :

/stockCompanies/update [symbol=unqdrg]

-------- output --------
<tr>
<td class="controlColumn">
<input name="symbols" value = "unqdrg" type="checkbox" class="itemCheckb
ox" id="symbol_unqdrg" />
</td>
<td>
------------------------
```

47863 (2) - Web Tests Session Expiration Errors

Synopsis

Nessus was logged out while running the web attacks.

Description

Nessus encountered trouble while running the web tests against the remote web server - test results may be incomplete.

Solution

Rescan with less parallelism or by requesting more session refresh, for example, by changing the following options in the scan policy :
- Preferences -> HTTP login page -> re-authenticate delay (seconds)
- Options -> Number of hosts in parallel (max_hosts)
- Options -> Number of checks in parallel (max_checks)

Risk Factor

None

Plugin Information:

Publication date: 2010/07/27, Modification date: 2011/03/19

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
- during the execution of virobot_linux_server_filescan_auth_bypass.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of cart32_file_retrieval.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of goscript_command_exec.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of plumtree_portal_user_info_disclosure.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of kerio_wrf_source_disclosure.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of silentstorm_xss.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of domino_traversal.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of db4web_dir_trav.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of netscape_publishing_expert_psuser.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of symantec_backup_exec_system_recovery_manager_multiple.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of fedora_ds_pass_disclosure.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of ibm_login_qs_xss.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of cyberoam_utm_console_detect.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of torture_cgi_local_file_inclusion.nasl, the
session expired 12 time(s) and re-authentication failed 12 time(s).
- during the execution of torture_cgi_script_injection.nasl, the
session expired 2 time(s) and re-authentication failed 2 time(s).
- during the execution of htsearch_sort_xss.nasl, [...]
```

iosr_client.cloudfoundry.com (tcp/443)

```
- during the execution of virobot_linux_server_filescan_auth_bypass.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of cart32_file_retrieval.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of kerio_wrf_source_disclosure.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of apache_mod_proxy_info_leak.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of silentstorm_xss.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of db4web_dir_trav.nasl, the
```

```
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of csSearch_cgi.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of symantec_backup_exec_system_recovery_manager_multiple.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of fedora_ds_pass_disclosure.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of groupwise_webaccess_userid_xss.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of apache_httponly_info_leak.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of torture_cgi_local_file_inclusion.nasl, the
session expired 34 time(s) and re-authentication failed 34 time(s).
- during the execution of torture_cgi_script_injection.nasl, the
session expired 2 time(s) and re-authentication failed 2 time(s).
- during the execution of htsearch_sort_xss.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of frontpage_chunked_overflow.nasl, the
session expired 1 time(s) and re-authentication failed 1 time(s).
- during the execution of saxopress_url_dir_traversal.nasl, th [...]
```

49704 (2) - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/10/04, Modification date: 2011/08/19

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
4 external URLs were gathered on this web server :
URL...                                  - Seen on...

http://ajax.googleapis.com/ajax/libs/jquery/1.7.1/jquery.min.js - /administrator/edit/9
http://ajax.googleapis.com/ajax/libs/jquery/1.9.1/jquery.min.js - /
http://code.jquery.com/jquery-latest.js - /administrator/edit/9
http://jzaefferer.github.com/jquery-validation/jquery.validate.js - /administrator/edit/9
```

iosr_client.cloudfoundry.com (tcp/443)

```
4 external URLs were gathered on this web server :
URL...                                  - Seen on...

http://ajax.googleapis.com/ajax/libs/jquery/1.7.1/jquery.min.js - /administrator/edit/9
http://ajax.googleapis.com/ajax/libs/jquery/1.9.1/jquery.min.js - /
http://code.jquery.com/jquery-latest.js - /administrator/edit/9
http://jzaefferer.github.com/jquery-validation/jquery.validate.js - /administrator/edit/9
```

10028 (1) - DNS Server BIND version Directive Remote Version Disclosure

Synopsis

It is possible to obtain the version number of the remote DNS server.

Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request, for the text 'version.bind' in the domain 'chaos'.
This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

It is possible to hide the version number of bind by using the 'version' directive in the 'options' section in named.conf

Risk Factor

None

References

XREF	OSVDB:23

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/05/24

Hosts

iosr_client.cloudfoundry.com (udp/53)

```
The version of the remote DNS server is :

unbound 1.4.17
```

10287 (1) - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Hosts

iosr_client.cloudfoundry.com (udp/0)

```
For your information, here is the traceroute from 192.168.203.41 to 173.243.49.35 :
192.168.203.41
192.168.192.1
173.243.49.35
```

10386 (1) - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.
Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/04/28, Modification date: 2011/10/20

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 302
rather than 404. The requested URL was :

    http://iosr_client.cloudfoundry.com/0p2zJmX3JrF4.html
```

10863 (1) - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/05/19, Modification date: 2012/04/02

Hosts

iosr_client.cloudfoundry.com (tcp/443)

```
Subject Name:

Country: US
State/Province: California
Locality: Palo Alto
Organization: VMware, Inc.
Organization Unit: Cloud Foundry
Common Name: *.cloudfoundry.com

Issuer Name:

Country: US
Organization: DigiCert Inc
Organization Unit: www.digicert.com
Common Name: DigiCert High Assurance CA-3

Serial Number: 0F D9 24 13 10 39 A5 6D 3B D7 DE A9 F3 DA 29 F0

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jun 18 00:00:00 2012 GMT
Not Valid After: Oct 05 12:00:00 2015 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B6 29 84 43 32 8C 7C 9F 4C CB 8B CB 72 A2 B0 8E 57 05 36
            0E A1 2E 0D ED 5D 87 24 DB 39 57 AF 1A AC 56 ED 48 AC E2 E6
            32 A5 25 FB C1 F3 54 15 FB 91 CB 51 2C 13 BF 0E 1C C7 C8 AC
            32 36 71 27 00 57 FF 94 81 95 2A B3 69 84 03 11 1E B0 9D 7B
            F0 EC EF A6 C6 5F 94 94 E9 58 F5 A9 58 D2 CE 73 8B 6E B9 42
            39 D6 B2 D5 7D 44 16 2C 0E D4 FF 77 1F B2 BB AC 41 C5 42 30
            CC 5C 9B 18 4C 82 D8 BF E6 96 69 2A 02 78 C0 82 0F B5 65 E5
            E6 96 EB 8B FD 89 2A 8F 61 54 E9 ED AA 83 64 9D 5F B3 60 15
            6F AB 49 14 BC 0E 18 84 D0 72 B2 97 13 51 35 7F AB 40 EF E7
            93 F5 79 71 62 AF 38 F1 66 59 4E FC BA 03 21 60 06 94 8D AB
            9F 25 BD 5D D2 0C 34 FD 13 0F 60 FE 55 B6 01 3A E0 8F 10 34
            63 8A 58 8C 58 D0 D4 D7 09 63 0E 80 BC 68 75 02 71 95 E3 F8
            0C A8 55 B5 1B 6E C1 DD 68 7E 32 63 EB C9 09 85 B9
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 66 7C 1B 43 88 66 62 A7 AC EA C5 2F B9 C2 D6 B5 5F A1 A7
           5C A5 60 B9 DD CC D8 E5 89 1D C7 55 E1 C2 F0 94 14 85 B7 24
           4B 8F E7 00 6D 88 CE 92 5F 50 C5 67 71 FA 53 D0 3E A9 42 78
           45 04 8C 73 76 6F 06 13 DB 78 A5 0D 8A 90 7A 0B 88 80 F0 3B
           70 5E 80 AB 83 A0 99 25 EF 1D A5 26 27 DF FE 7F EF 88 3C 18
           75 09 66 A4 FB 5C 44 76 AF E0 BC 75 6C 61 9A 20 DA B2 42 5E
```

```
04 26 D2 9E 14 0B 92 FC DE [...]
```

11002 (1) - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

http://en.wikipedia.org/wiki/Domain_Name_System

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information:

Publication date: 2003/02/13, Modification date: 2013/05/07

Hosts

iosr_client.cloudfoundry.com (udp/53)

11032 (1) - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/Predictable-Resource-Location

Solution

n/a

Risk Factor

None

References

XREF	OWASP:OWASP-CM-006

Plugin Information:

Publication date: 2002/06/26, Modification date: 2013/04/02

Hosts

iosr_client.cloudfoundry.com (tcp/443)

```
The following directories were discovered:
/login, /cgi-bin/eboard40/

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

11040 (1) - HTTP Reverse Proxy Detection

Synopsis

A transparent or reverse HTTP proxy is running on this port.

Description

This web server is reachable through a reverse HTTP proxy.

Solution

n/a

Risk Factor

None

STIG Severity

II

References

CVE	CVE-2004-2320
CVE	CVE-2005-3398
CVE	CVE-2005-3498
CVE	CVE-2007-3008
XREF	IAVT:2005-T-0043
XREF	CWE:200
XREF	CWE:79

Plugin Information:

Publication date: 2002/07/02, Modification date: 2012/08/18

Hosts

iosr_client.cloudfoundry.com (tcp/80)

```
The GET method revealed those proxies on the way to this web server :
HTTP/1.1     plus.ds14.agh.edu.pl:3128 (squid)
```

11153 (1) - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/11/18, Modification date: 2013/03/11

Hosts

iosr_client.cloudfoundry.com (tcp/3128)

```
A web server seems to be running on this port.
```

11936 (1) - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...), it is possible to guess the name of the remote operating system in use. It is also sometimes possible to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2013/04/01

Hosts

iosr_client.cloudfoundry.com (tcp/0)

```
Remote operating system : Linksys Wireless Access Point
Linux Kernel 2.6
Confidence Level : 59
Method : SinFP

Not all fingerprints could give a match.  If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org.  Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

HTTP:!:Server: nginx
SinFP:
   P1:B10113:F0x12:W5840:O0204ffff:M1460:
   P2:B10113:F0x12:W5792:O0204ffff0402080affffffff4445414401030307:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:5200_7_p=3128R
SMTP:!:554 Mozliwosc wysylania poczty z uzyciem portu 25 zostala zablokowana - prosze skorzystac z
 portu 587(TLS) lub 465(SSL)
SSLcert:!:i/CN:DigiCert High Assurance CA-3i/O:DigiCert Inci/OU:www.digicert.coms/
CN:*.cloudfoundry.coms/O:VMware, Inc.s/OU:Cloud Foundry
c2f6a71b63504587e99923ec64652da18674bc9e



The remote host is running one of these operating systems :
Linksys Wireless Access Point
Linux Kernel 2.6
```

12053 (1) - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the FQDN of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/02/11, Modification date: 2012/09/28

Hosts

iosr_client.cloudfoundry.com (tcp/0)

```
173.243.49.35 resolves as iosr_client.cloudfoundry.com.
```

18528 (1) - SMTP Server Connection Check

Synopsis

Nessus was able to connect to the remote SMTP server.

Description

Nessus was able to connect to the remote SMTP server and issue the HELO command.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/06/18, Modification date: 2011/03/11

Hosts

iosr_client.cloudfoundry.com (tcp/25)

```
The SMTP server on this port answered with a 554 code.
This means that it is permanently unavailable because the Nessus
server IP is not authorized, blacklisted or any other reason.

** Nessus tests will be incomplete. You may try to scan your MTA
** from an authorized IP or disable this server if you don't use it.
```

19506 (1) - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :
- The version of the plugin set
- The type of plugin feed (HomeFeed or ProfessionalFeed)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2013/05/31

Hosts

iosr_client.cloudfoundry.com (tcp/0)

```
Information about this scan :

Nessus version : 5.2.1
Plugin feed version : 201306090115
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.203.41
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 2
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : some_pairs
Web app tests -  Try all HTTP methods : no
Web app tests -  Maximum run time : 60 minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2013/6/9 14:25
Scan duration : 13490 sec
```

21643 (1) - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This script detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2012/10/16

Hosts

iosr_client.cloudfoundry.com (tcp/443)

```
Here is the list of SSL ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES(168)          Mac=SHA1
      DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES(168)          Mac=SHA1
      RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)           Mac=MD5
      RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)           Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES(168)          Mac=SHA1
      DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES(128)           Mac=SHA1
      DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES(256)           Mac=SHA1
      DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES(168)          Mac=SHA1
      AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES(128)           Mac=SHA1
      AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES(256)           Mac=SHA1
      RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)           Mac=MD5
      RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)           Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

25220 (1) - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Hosts

iosr_client.cloudfoundry.com (tcp/0)

35371 (1) - DNS Server hostname.bind Map Hostname Disclosure

Synopsis

The DNS server discloses the remote host name.

Description

It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

Solution

It may be possible to disable this feature. Consult the vendor's documentation for more information.

Risk Factor

None

Plugin Information:

Publication date: 2009/01/15, Modification date: 2011/09/14

Hosts

iosr_client.cloudfoundry.com (udp/53)

```
The remote host name is :

plus.ds14.agh.edu.pl
```

42799 (1) - Broken Web Servers

Synopsis

Tests on this web server have been disabled.

Description

The remote web server seems password protected or misconfigured. Further tests on it were disabled so that the whole scan is not slowed down.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/11/13, Modification date: 2011/08/17

Hosts

iosr_client.cloudfoundry.com (tcp/3128)

```
This web server was declared broken by :
 broken_web_server.nasl
for the following reasons :
 The server appears to speak HTTP/0.9 only.
 The server did not answer to a 'GET' HTTP request.
```

45590 (1) - Common Platform Enumeration (CPE)

Synopsis

It is possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2013/05/13

Hosts

iosr_client.cloudfoundry.com (tcp/0)

```
The remote operating system matched the following CPE :

  cpe:/o:linux:linux_kernel:2.6

Following application CPE matched on the remote system :

  cpe:/a:isc:bind:unbound
```

46180 (1) - Additional DNS Hostnames

Synopsis

Potential virtual hosts have been detected.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Different web servers may be hosted on name- based virtual hosts.

See Also

http://en.wikipedia.org/wiki/Virtual_hosting

Solution

If you want to test them, re-scan using the special vhost syntax, such as :
www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information:

Publication date: 2010/04/29, Modification date: 2013/01/21

Hosts

iosr_client.cloudfoundry.com (tcp/0)

```
The following hostnames point to the remote host:
  - cloudfoundry.com
```

51891 (1) - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/02/07, Modification date: 2012/04/19

Hosts

iosr_client.cloudfoundry.com (tcp/443)

```
This port supports resuming TLSv1 / SSLv3 sessions.
```

56984 (1) - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This script detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/01, Modification date: 2012/09/27

Hosts

iosr_client.cloudfoundry.com (tcp/443)

```
This port supports SSLv3/TLSv1.0/TLSv1.1.
```

57041 (1) - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

http://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/07, Modification date: 2012/04/02

Hosts

iosr_client.cloudfoundry.com (tcp/443)

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES(168)            Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES(168)            Mac=SHA1
      DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES(128)             Mac=SHA1
      DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES(256)             Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

58768 (1) - SSL Resume With Different Cipher Issue

Synopsis

The remote host allows resuming SSL sessions with a different cipher than the one originally negotiated.

Description

The SSL implementation on the remote host has been shown to allow a cipher other than the one originally negotiated when resuming a session. An attacker that sees (e.g. by sniffing) the start of an SSL connection may be able to manipulate session cache to cause subsequent resumptions of that session to use a cipher chosen by the attacker.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/04/17, Modification date: 2012/04/17

Hosts

iosr_client.cloudfoundry.com (tcp/443)

```
The server allowed the following session over SSLv3 to be resumed as follows :

  Session ID     : 067992d728927cf9fd48f60a4beb267fbd39ccf940f3b3f0fec05737681b8e1a
  Initial Cipher : SSL3_CK_RSA_RC4_128_SHA (0x0005)
  Resumed Cipher : SSL3_CK_RSA_DES_192_CBC3_SHA (0x000a)

The server allowed the following session over TLSv1 to be resumed as follows :

  Session ID     : eb29151f3f00d54e1f96e4ce070e3295c2787361e705a94b15be318f152d30fc
  Initial Cipher : TLS1_CK_RSA_WITH_RC4_128_SHA (0x0005)
  Resumed Cipher : SSL3_CK_RSA_DES_192_CBC3_SHA (0x000a)
```

62563 (1) - SSL Compression Methods Supported

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml

http://tools.ietf.org/html/rfc3749

http://tools.ietf.org/html/rfc3943

http://tools.ietf.org/html/rfc5246

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/10/16, Modification date: 2012/10/16

Hosts

iosr_client.cloudfoundry.com (tcp/443)

```
Nessus was able to confirm that the following compression method is
supported by the target :

  NULL (0x00)
```

66334 (1) - Patch Report

Synopsis

The remote host is missing several patches

Description

The remote host is missing one or several security patches.
This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Solution

Install the patches listed below

Risk Factor

None

Plugin Information:

Publication date: 2013/05/07, Modification date: 2013/06/04

Hosts

iosr_client.cloudfoundry.com (tcp/0)

```
. You need to take the following action:
[ DNS Server Recursive Query Cache Poisoning Weakness (10539) ]

+ Action to take: Restrict recursive queries to the hosts that should use this nameserver (such as
 those of the LAN connected to it).

If you are using bind 8, you can do this by using the instruction 'allow-recursion' in the
 'options' section of your named.conf.

If you are using bind 9, you can define a grouping of internal addresses using the 'acl' command.

Then, within the options block, you can explicitly state:
'allow-recursion { hosts_defined_in_acl }'

If you are using another name server, consult its documentation.
```