Summary

This document reports on the results of an automatic security scan. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Vendor security updates are not trusted.

Overrides are on. When a result has an override, this report uses the threat of the override.

Information on overrides is included in the report.

Notes are included in the report.

This report might not show details of all issues that were found. It only lists hosts that produced issues. Issues with the threat level "Log" are not shown. Issues with the threat level "Debug" are not shown. Issues with the threat level "False Positive" are not shown. Only results with a minimum QoD of 70 are shown.

This report contains all 8 results selected by the filtering described above. Before filtering there were 93 results.

All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC".

Scan started:	**Mon Aug 5 03:20:26 2019 UTC**
Scan ended:	Mon Aug 5 03:42:40 2019 UTC
Task:	SiyuanJi_home_wifi

Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive
192.168.1.104	Aug 5, 03:21:36	Aug 5, 03:34:46	1	2	1	0	0
192.168.1.1 (Linksys01270)	Aug 5, 03:20:42	Aug 5, 03:42:40	1	2	1	0	0
Total: 2			2	4	2	0	0

Results per Host

Host 192.168.1.104

Scanning of this host started at:	Mon Aug 5 03:21:36 2019 UTC
Number of results:	4

Port Summary for Host 192.168.1.104

Service (Port)	Threat Level
general/tcp	Low
9295/tcp	High

Security Issues for Host 192.168.1.104

High (CVSS: 10.0) 9295/tcp
NVT: Linksys WRT54G DoS (OID: 1.3.6.1.4.1.25623.1.0.11941)

Summary

It is possible to freeze the remote web server by sending an empty GET request.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

Solution type: VendorFix

Upgrade your firmware.

Affected Software/OS

This is know to affect Linksys WRT54G routers.

Vulnerability Detection Method

Details: Linksys WRT54G DoS (OID: 1.3.6.1.4.1.25623.1.0.11941)

Version used: 2019-04-24T07:26:10+0000

References

Other: http://www.zone-h.org/en/advisories/read/id=3523/

Medium (CVSS: 5.0) 9295/tcp
NVT: Webseal denial of service (OID: 1.3.6.1.4.1.25623.1.0.11089)

Summary

The remote web server dies when an URL ending with %2E is requested.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

An attacker may use this flaw to make your server crash continually.

Solution

Solution type: VendorFix

Upgrade your server or firewall it.

Affected Software/OS

Webseal version 3.8. Other versions or products might be affected as well.

Vulnerability Detection Method

Details: Webseal denial of service (OID: 1.3.6.1.4.1.25623.1.0.11089)

Version used: 2019-04-24T07:26:10+0000

References

CVE: CVE-2001-1191
BID: 3685

Medium (CVSS: 5.0) 9295/tcp
NVT: Polycom ViaVideo denial of service (OID: 1.3.6.1.4.1.25623.1.0.11825)

Summary

The remote web server locks up when several incomplete web requests are sent and the connections are kept open.

Vulnerability Detection Result

```
The remote web server locks up when several incomplete web
  requests are sent and the connections are kept open.

  However, it runs again when the connections are closed.
```

Solution

Solution type: VendorFix

Contact your vendor for a patch, upgrade your web server.

Vulnerability Insight

Some servers (e.g. Polycom ViaVideo) even run an endless loop, using much CPU on the machine. The scanner has no way to test this, but you'd better check your machine.

Vulnerability Detection Method

Details: Polycom ViaVideo denial of service (OID: 1.3.6.1.4.1.25623.1.0.11825)

Version used: 2019-04-11T14:06:24+0000

References

CVE: CVE-2002-1906
BID: 5962

Low (CVSS: 2.6) general/tcp
NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 3366211801
Packet 2: 1067549825
```

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

Solution type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

Affected Software/OS

TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight

The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

Version used: $Revision: 14310 $

References

Other: http://www.ietf.org/rfc/rfc1323.txt
http://www.microsoft.com/en-us/download/details.aspx?id=9152

Host 192.168.1.1

Scanning of this host started at:	Mon Aug 5 03:20:42 2019 UTC
Number of results:	4

Port Summary for Host 192.168.1.1

Service (Port)	Threat Level
10080/tcp	High
general/tcp	Low
80/tcp	Medium

Security Issues for Host 192.168.1.1

High (CVSS: 7.5) 10080/tcp
NVT: Lighttpd Multiple vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.802072)

Summary

This host is running Lighttpd and is prone to multiple vulnerabilities

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to execute arbitrary SQL commands and remote attackers to read arbitrary files via hostname.

Solution

Solution type: VendorFix

Upgrade to 1.4.35 or later.

Affected Software/OS

Lighttpd version before 1.4.35

Vulnerability Insight

- mod_mysql_vhost module not properly sanitizing user supplied input passed via the hostname.
- mod_evhost and mod_simple_vhost modules not properly sanitizing user supplied input via the hostname.

Vulnerability Detection Method

Send a crafted HTTP GET request and check whether it responds with error message.

Details: Lighttpd Multiple vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.802072)

Version used: $Revision: 11867 $

References

CVE:	CVE-2014-2323, CVE-2014-2324
BID:	66153, 66157
CERT:	CB-K14/0300, DFN-CERT-2014-0311
Other:	http://seclists.org/oss-sec/2014/q1/561 http://download.lighttpd.net/lighttpd/security/lighttpd_sa_2014_01.txt http://www.lighttpd.net/download

Medium (CVSS: 5.0) 80/tcp
NVT: Missing `httpOnly` Cookie Attribute (OID: 1.3.6.1.4.1.25623.1.0.105925)

Summary

The application is missing the 'httpOnly' cookie attribute

Vulnerability Detection Result

```
The cookies:

Set-Cookie: ui-proxy-path=***replaced***; path=/; domain=Linksys01270

are missing the "httpOnly" attribute.
```

Solution

Solution type: Mitigation

Set the 'httpOnly' attribute for any session cookie.

Affected Software/OS

Application with session handling in cookies.

Vulnerability Insight

The flaw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Vulnerability Detection Method

Check all cookies sent by the application for a missing 'httpOnly' attribute

Details: Missing `httpOnly` Cookie Attribute (OID: 1.3.6.1.4.1.25623.1.0.105925)

Version used: $Revision: 5270 $

References

Other:	https://www.owasp.org/index.php/HttpOnly https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)

Medium (CVSS: 4.3) 80/tcp
NVT: Apache Web Server ETag Header Information Disclosure Weakness (OID: 1.3.6.1.4.1.25623.1.0.103122)

Summary

A weakness has been discovered in Apache web servers that are configured to use the FileETag directive.

Vulnerability Detection Result

```
Information that was gathered:
Inode: 400041
Size: 8518
```

Impact

Exploitation of this issue may provide an attacker with information that may be used to launch further attacks against a target network.

Solution

Solution type: VendorFix

OpenBSD has released a patch that addresses this issue. Inode numbers returned from the server are now encoded using a private hash to avoid the release of sensitive information.

Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare. Please see the attached Technical Information Document for further details.

Vulnerability Detection Method

Due to the way in which Apache generates ETag response headers, it may be possible for an attacker to obtain sensitive information regarding server files. Specifically, ETag header fields returned to a client contain the file's inode number.

Details: Apache Web Server ETag Header Information Disclosure Weakness (OID: 1.3.6.1.4.1.25623.1.0.103122)

Version used: 2019-05-13T14:05:09+0000

References

CVE:	CVE-2003-1418
BID:	6939
CERT:	CB-K17/1750, CB-K17/0896, CB-K15/0469, DFN-CERT-2017-1821, DFN-CERT-2017-0925, DFN-CERT-2015-0495
Other:	https://www.securityfocus.com/bid/6939
	http://httpd.apache.org/docs/mod/core.html#fileetag
	http://www.openbsd.org/errata32.html
	http://support.novell.com/docs/Tids/Solutions/10090670.html

Low (CVSS: 2.6) general/tcp
NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 33195905
Packet 2: 33196015
```

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

Solution type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

Affected Software/OS

TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight

The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

Version used: $Revision: 14310 $

References

Other: http://www.ietf.org/rfc/rfc1323.txt
http://www.microsoft.com/en-us/download/details.aspx?id=9152

This file was automatically generated.