Scan Report

December 1, 2018

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Immediate scan of IP 192.168.1.134”. The scan started at Sat Dec 1 15:57:01 2018 UTC and ended at Sat Dec 1 16:11:40 2018 UTC. 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.

Contents

1 Result Overview **2**

2 Results per Host **2**

2.1 192.168.1.134 2

2.1.1 High 80/tcp 2

2.1.2 High 8080/tcp 3

2.1.3 Medium 80/tcp 4

2.1.4 Low general/tcp 5

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.1.134	2	1	1	0	0
Total: 1	2	1	1	0	0

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 4 results selected by the filtering described above. Before filtering there were 38 results.

2 Results per Host

2.1 192.168.1.134

Host scan start	Sat Dec 1 15:57:05 2018 UTC
Host scan end	Sat Dec 1 16:11:40 2018 UTC

Service (Port)	Threat Level
80/tcp	High
8080/tcp	High
80/tcp	Medium
general/tcp	Low

2.1.1 High 80/tcp

High (CVSS: 9.0)
NVT: HTTP Brute Force Logins With Default Credentials Reporting

Summary
It was possible to login into the remote Web Application using default credentials.

. . . continues on next page . . .

. . . continued from previous page . . .

As the NVT 'HTTP Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108041) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result

```
It was possible to login with the following credentials <Url>:<User>:<Password>:
↪<HTTP status code>
http://192.168.1.134/home.asp:admin:admin:HTTP/1.1 404 Site or Page Not Found
```

Solution

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Try to login with a number of known default credentials via HTTP Basic Auth.

Details: `HTTP Brute Force Logins With Default Credentials Reporting`

OID:1.3.6.1.4.1.25623.1.0.103240

Version used: `$Revision: 11663 $`

[return to 192.168.1.134]

2.1.2 High 8080/tcp

High (CVSS: 7.5)

NVT: Lighttpd Multiple vulnerabilities

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.

. . . continues on next page . . .

. . . continued from previous page . . .

- 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
Other:
  URL:http://seclists.org/oss-sec/2014/q1/561
   URL:http://download.lighttpd.net/lighttpd/security/lighttpd_sa_2014_01.txt
   URL:http://www.lighttpd.net/download
```

[return to 192.168.1.134]

2.1.3 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result

```
The following URLs requires Basic Authentication (URL:realm name):
http://192.168.1.134/:"GoAhead"
```

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.

The script is currently checking the following:

- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'

Details: `Cleartext Transmission of Sensitive Information via HTTP`

OID:1.3.6.1.4.1.25623.1.0.108440

Version used: `$Revision: 10726 $`

References

```
Other:
  URL:https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_S
↪ession_Management
   URL:https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
   URL:https://cwe.mitre.org/data/definitions/319.html
```

[return to 192.168.1.134]

2.1.4 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

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: 4294957047
Packet 2: 4294957331
```

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.

. . . continues on next page . . .

. . . continued from previous page . . .

See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

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: 10411 $`

References

```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
```

[return to 192.168.1.134]

This file was automatically generated.