Scan Report

October 9, 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 "Complete scan for iSignif". The scan started at Tue Oct 9 16:13:35 2018 UTC and ended at Tue Oct 9 16:42:11 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

Host	High	Medium	Low	Log	False Positive
51.75.24.68 isignif.fr	1	0	1	0	0
Total: 1	1	0	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 2 results selected by the filtering described above. Before filtering there were 46 results.

2 Results per Host

2.1 51.75.24.68

Host scan start	Tue Oct 9 16:13:45 2018 UTC
Host scan end	Tue Oct 9 16:42:11 2018 UTC

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

2.1.1 High 80/tcp

High (CVSS: 7.5)
NVT: Incomplete basic authentication DoS

Summary
It was possible to kill the web server by sending an invalid request with an incomplete Basic authentication.
A cracker may exploit this vulnerability to make your web server crash continually or even execute arbirtray code on your system.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
upgrade your software or protect it with a filtering reverse proxy

Vulnerability Detection Method
Details: `Incomplete basic authentication DoS`
OID:1.3.6.1.4.1.25623.1.0.12200
Version used: `$Revision: 9348 $`

[return to 51.75.24.68]

2.1.2 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: 1236156017
Packet 2: 1236157043
```

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 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.

... continues on next page ...

... continued from previous page ...

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 51.75.24.68]