Scan Report

February 26, 2015

Summary

This document reports on the results of an automatic security scan. The scan started at Thu Feb 26 13:34:37 2015 UTC and ended at Thu Feb 26 13:35:45 2015 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	Most Severe Result(s)	High	Medium	Low	Log	False Positives
192.168.1.10	Severity: Low	0	0	1	6	0
Total: 1		0	0	1	6	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
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 "Debug" are not shown.

This report contains all 7 results selected by the filtering described above. Before filtering there were 7 results.

2 Results per Host

2.1 192.168.1.10

Host scan start	Thu Feb 26 13:35:18 2015 UTC
Host scan end	Thu Feb 26 13:35:45 2015 UTC

Service (Port)	Threat Level
domain (53/udp)	Low
domain (53/udp)	Log
general/HOST-T	Log
general/icmp	Log
general/tcp	Log

2.1.1 Low domain (53/udp)

Low (CVSS: 5.0)
NVT: Determine which version of BIND name daemon is running

```
BIND 'NAMED' is an open-source DNS server from ISC.org.
Many proprietary DNS servers are based on BIND source code.
The BIND based NAMED servers (or DNS servers) allow remote users
to query for version and type information.  The query of the CHAOS
TXT record 'version.bind', will typically prompt the server to send
the information back to the querying source.
The remote bind version is : 9.7.0-P1
Solution :
```

...continues on next page ...

... continued from previous page ...

```
Using the 'version' directive in the 'options' section will block
the 'version.bind' query, but it will not log such attempts.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10028

[return to 192.168.1.10]

2.1.2 Log domain (53/udp)

Log (CVSS: 0.0)
NVT: DNS Server Detection

```
 Summary:
 A DNS Server is running at this Host.
A Name Server translates domain names into IP addresses. This makes it
possible for a user to access a website by typing in the domain name instead of
the website's actual IP address.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100069

[return to 192.168.1.10]

2.1.3 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

```
traceroute:192.168.1.1,192.168.1.10
TCP ports:
UDP ports:
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810003

[return to 192.168.1.10]

2.1.4 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

```
Summary:
The remote host responded to an ICMP timestamp request. The Timestamp Reply is
an ICMP message which replies to a Timestamp message. It consists of the
originating timestamp sent by the sender of the Timestamp as well as a receive
timestamp and a transmit timestamp. This information could theoretically be used
to exploit weak time-based random number generators in other services.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103190

References

```
CVE: CVE-1999-0524
Other:
  URL:http://www.ietf.org/rfc/rfc0792.txt
```

[return to 192.168.1.10]

2.1.5 Log general/tcp

Log (CVSS: 0.0)
NVT: Checks for open udp ports

```
Open UDP ports: [None found]
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103978

Log (CVSS: 0.0)
NVT: Traceroute

```
Here is the route from 192.168.1.1 to 192.168.1.10:
192.168.1.1
192.168.1.10
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.51662

Log (CVSS: 0.0)
NVT: Checks for open tcp ports

```
Open TCP ports: [None found]
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900239

[return to 192.168.1.10]
