

Scan Report

February 26, 2015

Summary

This document reports on the results of an automatic security scan. The scan started at Thu Feb 26 13:24:38 2015 UTC and ended at Thu Feb 26 13:25:49 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	2
2	Results per Host	2
2.1	192.168.1.10	2
2.1.1	Log domain (53/udp)	2
2.1.2	Log general/CPE-T	3
2.1.3	Log general/icmp	3

1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
192.168.1.10	Severity: Log	0	0	0	3	0
Total: 1		0	0	0	3	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 3 results selected by the filtering described above. Before filtering there were 3 results.

2 Results per Host

2.1 192.168.1.10

Host scan start Thu Feb 26 13:25:12 2015 UTC

Host scan end Thu Feb 26 13:25:49 2015 UTC

Service (Port)	Threat Level
domain (53/udp)	Log
general/CPE-T	Log
general/icmp	Log

2.1.1 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

[\[return to 192.168.1.10 \]](#)

2.1.2 Log general/CPE-T

Log (CVSS: 0.0) NVT: CPE Inventory
192.168.1.10 cpe:/o:linux:kernel
OID of test routine: 1.3.6.1.4.1.25623.1.0.810002

[\[return to 192.168.1.10 \]](#)

2.1.3 Log general/icmp

Log (CVSS: 0.0) NVT: ICMP Timestamp Detection
<p>Summary:</p> <p>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.</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.103190</p>
<p>References</p> <p>CVE: CVE-1999-0524</p> <p>Other:</p> <p>URL:http://www.ietf.org/rfc/rfc0792.txt</p>

[\[return to 192.168.1.10 \]](#)