Scan Report

November 3, 2019

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 "Discovery". The scan started at and ended at . 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
192.168.0.57	1	1	0	0	0
Total: 1	1	1	0	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 72 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.0.57	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 192.168.0.57

Host scan start
Host scan end

Service (Port)	Threat Level
514/tcp	High
21/tcp	Medium

2.1.1 High 514/tcp

High (CVSS: 7.5)
NVT: rsh Unencrypted Cleartext Login

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This remote host is running a rsh service.

Vulnerability Detection Result

```
The rsh service is misconfigured so it is allowing conntections without a passwo
↪rd or with default root:root credentials.
```

Solution

Solution type: Mitigation

Disable the rsh service and use alternatives like SSH instead.

Vulnerability Insight

rsh (remote shell) is a command line computer program which can execute shell commands as another user, and on another computer across a computer network.

Vulnerability Detection Method

Details: `rsh Unencrypted Cleartext Login`

OID:1.3.6.1.4.1.25623.1.0.100080

Version used: `$Revision: 13010 $`

References

```
Other:
  URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651
```

[return to 192.168.0.57]

2.1.2 Medium 21/tcp

Medium (CVSS: 6.4)
NVT: Anonymous FTP Login Reporting

Summary

Reports if the remote FTP Server allows anonymous logins.

Vulnerability Detection Result

```
It was possible to login to the remote FTP service with the following anonymous
↪account(s):
anonymous:anonymous@example.com
ftp:anonymous@example.com
```

Impact

Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to:

- gain access to sensitive files
- upload or delete files.

Solution

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: Mitigation
If you do not want to share files, you should disable anonymous logins.

Vulnerability Insight

A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.

Vulnerability Detection Method

Details: `Anonymous FTP Login Reporting`
OID:1.3.6.1.4.1.25623.1.0.900600
Version used: `$Revision: 12030 $`

References

```
Other:
  URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497
```

[return to 192.168.0.57]

This file was automatically generated.