Scan Report

July 1, 2022

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 "Scan Kali01". The scan started at Fri Jul 1 14:42:28 2022 UTC and ended at Fri Jul 1 14:48:32 2022 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
192.168.2.21	0	1	0	0	0
Total: 1	0	1	0	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
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.
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 result 1 of the 1 results selected by the filtering above. Before filtering there were 98 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.2.21	SSH	Success	Protocol SSH, Port 22, User kali

2 Results per Host

2.1 192.168.2.21

Host scan start	Fri Jul 1 14:43:00 2022 UTC
Host scan end	Fri Jul 1 14:48:28 2022 UTC

Service (Port)	Threat Level
general/tcp	Medium

2.1.1 Medium general/tcp

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

. . . continues on next page . . .

... continued from previous page ...

cpe:/a:jquery:jquery:3.6.0
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)

Summary
jQuery is vulnerable to Cross-site Scripting (XSS) attacks.

Vulnerability Detection Result
Installed version: 1.8.3
Fixed version: 1.9.0
Installation
path / port: /usr/share/faraday/server/www/script/jquery.js

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: jQuery < 1.9.0 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: 2021-06-11T08:43:18Z

Product Detection Result
Product: cpe:/a:jquery:jquery:3.6.0
Method: jQuery Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.150658)

References
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2020-0590

[return to 192.168.2.21]
