WebAuthn would allow a user to sign a challenge on a webpage with an invalid TLS certificate

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-6433
State	PUBLISHED
Assigner	mozilla
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-06-24 13:15:24 UTC
Updated	2026-04-13 15:17:07 UTC
Description	If a user visited a webpage with an invalid TLS certificate, and granted an exception, the webpage was able to provide a We

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from ADP

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000630000 probability, percentile 0.195630000 (date 2026-04-15)

Problem Types: CWE-295 | CWE-295 CWE-295 Improper Certificate Validation

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mozilla	Firefox	unaffected 140 * rpm	Not specified
CNA	Mozilla	Thunderbird	unaffected 140 * rpm	Not specified

References

Reference	Source	Link	Tags
www.mozilla.org/security/advisories/mfsa2025-51	security@mozilla.org	www.mozilla.org	Vendor Advisory
www.mozilla.org/security/advisories/mfsa2025-54	security@mozilla.org	www.mozilla.org	
bugzilla.mozilla.org/show_bug.cgi	security@mozilla.org	bugzilla.mozilla.org	Permissions Required
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Simon (en)

There are currently no legacy QID mappings associated with this CVE.