Downloading of OpenPGP keys from WKD used incorrect padding

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

Summary

CVE	CVE-2025-26695
State	PUBLISHED
Assigner	mozilla
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-03-10 19:15:40 UTC
Updated	2026-04-13 15:16:54 UTC
Description	When requesting an OpenPGP key from a WKD server, an incorrect padding size was used and a network observer could

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from ADP

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

Problem Types: NVD-CWE-noinfo | CWE-noinfo Not enough information

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
Low

Privileges Required
Low

User Interaction
None

Scope
Unchanged

Confidentiality
Low

Integrity
Low

Availability

Low

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

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mozilla	Thunderbird	unaffected 128.8 128.* rpm	Not specified
CNA	Mozilla	Thunderbird	unaffected 136 * rpm	Not specified

References

Reference	Source	Link	Tags
www.mozilla.org/security/advisories/mfsa2025-17	security@mozilla.org	www.mozilla.org	Vendor Advisory
www.mozilla.org/security/advisories/mfsa2025-18	security@mozilla.org	www.mozilla.org	Vendor Advisory
bugzilla.mozilla.org/show_bug.cgi	security@mozilla.org	bugzilla.mozilla.org	Issue Tracking
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: Daniel Huigens (en)

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