CVE-2014-1558

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

Summary

CVE	CVE-2014-1558
State	PUBLISHED
Assigner	mozilla
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-23 11:12:43 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Mozilla Firefox before 31.0 and Thunderbird before 31.0 allow remote attackers to cause a denial of service (X.509 certifica

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:N/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:M/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

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

Application	Mozilla	Thunderbird	24.0	All	All	All
Application	Mozilla	Thunderbird	24.0.1	All	All	All
Application	Mozilla	Thunderbird	24.1	All	All	All
Application	Mozilla	Thunderbird	24.1.1	All	All	All
Application	Mozilla	Thunderbird	24.2	All	All	All
Application	Mozilla	Thunderbird	24.3	All	All	All
Application	Mozilla	Thunderbird	24.4	All	All	All
Application	Mozilla	Thunderbird	24.5	All	All	All
Application	Mozilla	Thunderbird	24.6	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
Gentoo Security
MFSA 2014-65: Certificate parsing broken by non-standard character encoding
Security Advisory SA60628 - SUSE update for MozillaFirefox - Secunia
Mozilla Thunderbird Multiple Flaws Let Remote Users Deny Service and Execute Arbitrary Code - SecurityTracker
Access Denied
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Deny Service, and Spoof User Interface Elements - SecurityTracker
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

CVE.report and Source URL Uptime Status status.cve.report