CVE-2016-1935

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

Summary

CVE	CVE-2016-1935
State	PUBLISHED
Assigner	mozilla
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-01-31 18:59:03 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Buffer overflow in the BufferSubData function in Mozilla Firefox before 44.0 and Firefox ESR 38.x before 38.6 allows remote

Risk And Classification

Primary CVSS: v3.0 8.8 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Problem Types: CWE-119 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	9.3		AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	38.0	All	All	All
Application	Mozilla	Firefox	38.1.0	All	All	All
Application	Mozilla	Firefox	38.2.0	All	All	All
Application	Mozilla	Firefox	38.3.0	All	All	All
Application	Mozilla	Firefox	38.4.0	All	All	All
Application	Mozilla	Firefox	38.5.0	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Oracle	Linux	5.0	All	All	All
Operating System	Oracle	Linux	6	All	All	All
Operating System	Oracle	Linux	7	All	All	All

Vendor Declared Affected Products

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

References

Reference
Debian -- Security Information -- DSA-3457-1 iceweasel
openSUSE-SU-2016:0492-1: moderate: Security update for MozillaThunderbir
USN-2904-1: Thunderbird vulnerabilities | Ubuntu
Red Hat Customer Portal
Red Hat Customer Portal
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Spoof the Address Bar, Bypass Security Restrictions, and Deny Ser
openSUSE-SU-2016:0488-1: moderate: Security update for Thunderbird
Buffer overflow in WebGL after out of memory allocation — Mozilla
[security-announce] openSUSE-SU-2016:0306-1: important: Security update
Debian -- Security Information -- DSA-3491-1 icedove
1220450 - (CVE-2016-1935) global-buffer-overflow (write) at BufferSubData
[security-announce] SUSE-SU-2016:0338-1: important: Security update for
Mozilla Firefox CVE-2016-1935 Buffer Overflow Vulnerability
Mozilla Products: Multiple vulnerabilities (GLSA 201605-06) — Gentoo security
[security-announce] openSUSE-SU-2016:0310-1: important: Security update
[security-announce] openSUSE-SU-2016:0309-1: important: Security update
USN-2880-1: Firefox vulnerabilities | Ubuntu
Oracle Linux Bulletin - January 2016
USN-2880-2: Firefox regression | Ubuntu
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.