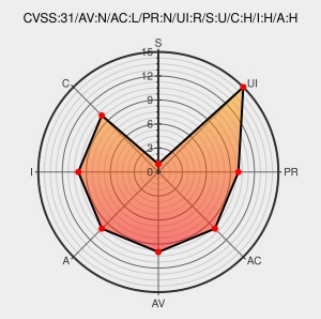
CVE-2019-17005

Published on: 01/08/2020 12:00:00 AM UTC

Last Modified on: 04/08/2022 02:31:00 PM UTC

CVE-2019-17005

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

The plain text serializer used a fixed-size array for the number of <ol> elements it could process; however it was possible to overflow the static-sized array leading to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.3, Firefox ESR < 68.3, and Firefox < 71.

CVE-2019-17005 has been assigned by security@mozilla.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Mozilla** - **Thunderbird** version **before 68.3**

Affected Vendor/Software: **Mozilla** - **Firefox ESR** version **before 68.3**

Affected Vendor/Software: **Mozilla** - **Firefox** version **before 71**

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Mozilla Thunderbird: Multiple vulnerabilities (GLSA 202003-10) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202003-10
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2020:0292
Mozilla Firefox: Multiple vulnerabilities (GLSA 202003-02) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202003-02
Security Vulnerabilities fixed in - Firefox 71 — Mozilla	Vendor Advisory www.mozilla.org text/html	CONFIRM www.mozilla.org/security/advisories/mfsa2019-36/
Security Vulnerabilities fixed in - Thunderbird 68.3 — Mozilla	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM www.mozilla.org/security/advisories/mfsa2019-38/
[security-announce] openSUSE-SU-2020:0003-1: important: Security update	Issue Tracking Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0003
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2020:0295
[security-announce] openSUSE-SU-2020:0002-1: important: Security update	Issue Tracking Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0002
USN-4335-1: Thunderbird vulnerabilities | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-4335-1
Security Vulnerabilities fixed in - Firefox ESR 68.3 — Mozilla	Vendor Advisory www.mozilla.org text/html	CONFIRM www.mozilla.org/security/advisories/mfsa2019-37/
1584170 - (CVE-2019-17005) Access heap-allocated array with index out of bounds in `nsPlainTextSerializer`	Permissions Required bugzilla.mozilla.org text/html	MISC bugzilla.mozilla.org/show_bug.cgi?id=1584170
USN-4241-1: Thunderbird vulnerabilities | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-4241-1

Related QID Numbers

500924 Alpine Linux Security Update for firefox-esr

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All

Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

- cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:esm:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:19.10:*:*:*:*:*:*:*:
- cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:*:
- cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:*:
- cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*:*:*:
- cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*:*:*:
- cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:*:*:*:
- cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:*:*:*:
- cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:*:
- cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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