CVE-2024-4367

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

Summary

CVE	CVE-2024-4367
State	PUBLISHED
Assigner	mozilla
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-14 18:15:12 UTC
Updated	2026-05-12 12:17:19 UTC
Description	A type check was missing when handling fonts in PDF.js, which would allow arbitrary JavaScript execution in the PDF.js co

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

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

EPSS: 0.377620000 probability, percentile 0.972450000 (date 2026-05-12)

Problem Types: NVD-CWE-noinfo | CWE-754 | Arbitrary JavaScript execution in PDF.js | CWE-754 CWE-754 Improper Check for Unusual or Exceptional Conditions

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	5.6	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.6	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	All	All	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	-	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision10	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision11	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision12	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision13	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision14	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision15	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision16	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision17	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision18	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision19	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision20	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision21	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision22	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision23	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision24	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision25	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision26	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision27	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision28	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision29	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision3	All	All

Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision30	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision31	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision32	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision33	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision34	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision35	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision36	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision37	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision38	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision39	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision4	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision40	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision41	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision42	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision43	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision44	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision5	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision6	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision7	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision8	All	All
Application	Open-xchange	Open-xchange Appsuite Frontend	7.10.6	revision9	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mozilla	Firefox	affected unspecified 126 custom	Not specified
CNA	Mozilla	Firefox ESR	affected unspecified 115.11 custom	Not specified
CNA	Mozilla	Thunderbird	affected unspecified 115.11 custom	Not specified
ADP	Mozilla	Thunderbird	affected 115.11 custom	Not specified
ADP	Mozilla	Firefox	affected 126 custom	Not specified
ADP	Mozilla	Firefox Esr	affected 115.11 custom	Not specified
ADP	Siemens	Teamcenter V2312	affected V2312.0009 custom	Not specified
ADP	Siemens	Teamcenter V2406	affected V2406.0006 custom	Not specified
ADP	Siemens	Teamcenter V2512	unaffected * custom	Not specified

References

Reference	Source	Link

lists.debian.org/debian-lts-announce/2024/05/msg00010.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
seclists.org/fulldisclosure/2024/Aug/30	af854a3a-2127-422b-91ae-364da2661108	seclists.org
www.exploit-db.com/exploits/52273	af854a3a-2127-422b-91ae-364da2661108	www.exploit-db.c
www.mozilla.org/security/advisories/mfsa2024-22	af854a3a-2127-422b-91ae-364da2661108	www.mozilla.org
www.mozilla.org/security/advisories/mfsa2024-23	af854a3a-2127-422b-91ae-364da2661108	www.mozilla.org
codeanlabs.com/blog/research/cve-2024-4367-arbitrary-js-execution-in-pdf-js	af854a3a-2127-422b-91ae-364da2661108	codeanlabs.com
cert-portal.siemens.com/productcert/html/ssa-827383.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.sieme
bugzilla.mozilla.org/show_bug.cgi	af854a3a-2127-422b-91ae-364da2661108	bugzilla.mozilla.c
github.com/gogs/gogs/issues/7928	af854a3a-2127-422b-91ae-364da2661108	github.com
www.mozilla.org/security/advisories/mfsa2024-21	af854a3a-2127-422b-91ae-364da2661108	www.mozilla.org
lists.debian.org/debian-lts-announce/2024/05/msg00012.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
github.com/mozilla/pdf.js/releases/tag/v4.2.67	af854a3a-2127-422b-91ae-364da2661108	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Thomas Rinsma of Codean Labs (en)

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