Xerte Online Toolkits File Upload RCE via elfinder Connector

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

Summary

CVE	CVE-2026-34415
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 19:17:04 UTC
Updated	2026-04-22 21:18:45 UTC
Description	Xerte Online Toolkits versions 3.15 and earlier contain an incomplete input validation vulnerability in the elFinder connector

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-184 | CWE-184 CWE-184 Incomplete List of Disallowed Inputs

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S
3.1	disclosure@vulncheck.com	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Thexerteproject	Xerteonlinetoolkits	affected 3.15.0 semver	Not specified
CNA	Thexerteproject	Xerteonlinetoolkits	affected 3.14.0 semver	Not specified
CNA	Thexerteproject	Xerteonlinetoolkits	affected 3.13.0 semver	Not specified
CNA	Thexerteproject	Xerteonlinetoolkits	affected 02661be88cc369325ea01b508086bde7fbfec805 git	Not specified

CNA	Thexerteproject	Xerteonlinetoolkits	affected 17e4f945fe6a3400fa88c01eda18c1075ee4a212 git	Not specified
CNA	Thexerteproject	Xerteonlinetoolkits	affected 507d55c5e91bf9310b5b1c7fad8aebfef902ad23 git	Not specified

References

Reference	Source	Link	Tags
github.com/thexerteproject/xerteonlinetoolkits/issues/1527	disclosure@vulncheck.com	github.com	
github.com/thexerteproject/xerteonlinetoolkits/commit/02661be88cc369325e...	disclosure@vulncheck.com	github.com	
github.com/thexerteproject/xerteonlinetoolkits/commit/17e4f945fe6a3400fa...	disclosure@vulncheck.com	github.com	
github.com/thexerteproject/xerteonlinetoolkits/commit/507d55c5e91bf9310b...	disclosure@vulncheck.com	github.com	
xerte.org.uk/xertetoolkits_3.15_ChangeLog.html	disclosure@vulncheck.com	xerte.org.uk	
www.vulncheck.com/advisories/xerte-online-toolkits-file-upload-rce-via-elfinder...	disclosure@vulncheck.com	www.vulncheck.com	
xerte.org.uk/index.php/en/downloads-1/category/3-xerte-online-toolkits	disclosure@vulncheck.com	xerte.org.uk	
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

Vendor Comments And Credit

Discovery Credit

CNA: bootstrapbool (en)

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