



# Xerte Online Toolkits Path Traversal via connector.php

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-34414
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulnCheck
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-22 19:17:04 UTC
<b>Updated</b>	2026-04-22 21:18:45 UTC
<b>Description</b>	Xerte Online Toolkits versions 3.15 and earlier contain a relative path traversal vulnerability in the elFinder connector endpoint

## Risk And Classification

**Primary CVSS:** v4.0 7.1 HIGH from disclosure@vulncheck.com

**CVSS:**4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:H/VA:N/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-22 | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:H/VA:N/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:H/VA:N/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	disclosure@vulncheck.com	Primary	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N

## CVSS v4.0 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Attack Requirements

**None**

Privileges Required

**Low**

User Interaction

**None**

Confidentiality

Low

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:H/VA:N/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/MSX: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

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

High

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Thexerteproject</a>	<a href="#">Xerteonlinetoolkits</a>	affected 3.15.0 semver	Not specified
CNA	<a href="#">Thexerteproject</a>	<a href="#">Xerteonlinetoolkits</a>	affected 3.14.0 semver	Not specified
CNA	<a href="#">Thexerteproject</a>	<a href="#">Xerteonlinetoolkits</a>	affected 3.13.0 semver	Not specified
CNA	<a href="#">Thexerteproject</a>	<a href="#">Xerteonlinetoolkits</a>	affected 02661be88cc369325ea01b508086bde7fbfec805 git	Not specified
CNA	<a href="#">Thexerteproject</a>	<a href="#">Xerteonlinetoolkits</a>	affected 17c4f045f6624006e88e01cda18e1075ee4e010 git	Not specified

CNA	<a href="#">thexerteproject</a>	<a href="#">xerteonlinetoolkits</a>	affected 17e4f945fe6a3400fa86c01eda18c1075ee4a212 git	not specified
CNA	<a href="#">Thexerteproject</a>	<a href="#">Xerteonlinetoolkits</a>	affected 507d55c5e91bf9310b5b1c7fad8aebfef902ad23 git	Not specified

## References

Reference	Source	Link	Tag
<a href="https://github.com/thexerteproject/xerteonlinetoolkits/issues/1527">github.com/thexerteproject/xerteonlinetoolkits/issues/1527</a>	disclosure@vulncheck.com	<a href="https://github.com">github.com</a>	
<a href="https://github.com/thexerteproject/xerteonlinetoolkits/commit/02661be88cc369325e...">github.com/thexerteproject/xerteonlinetoolkits/commit/02661be88cc369325e...</a>	disclosure@vulncheck.com	<a href="https://github.com">github.com</a>	
<a href="https://www.vulncheck.com/advisories/xerte-online-toolkits-path-traversal-via-connector...">www.vulncheck.com/advisories/xerte-online-toolkits-path-traversal-via-connector...</a>	disclosure@vulncheck.com	<a href="https://www.vulncheck.com">www.vulncheck.com</a>	
<a href="https://github.com/thexerteproject/xerteonlinetoolkits/commit/17e4f945fe6a3400fa...">github.com/thexerteproject/xerteonlinetoolkits/commit/17e4f945fe6a3400fa...</a>	disclosure@vulncheck.com	<a href="https://github.com">github.com</a>	
<a href="https://github.com/thexerteproject/xerteonlinetoolkits/commit/507d55c5e91bf9310b...">github.com/thexerteproject/xerteonlinetoolkits/commit/507d55c5e91bf9310b...</a>	disclosure@vulncheck.com	<a href="https://github.com">github.com</a>	
<a href="https://xerte.org.uk/xertetoolkits_3.15_ChangeLog.html">xerte.org.uk/xertetoolkits_3.15_ChangeLog.html</a>	disclosure@vulncheck.com	<a href="https://xerte.org.uk">xerte.org.uk</a>	
<a href="https://xerte.org.uk/index.php/en/downloads-1/category/3-xerte-online-toolkits">xerte.org.uk/index.php/en/downloads-1/category/3-xerte-online-toolkits</a>	disclosure@vulncheck.com	<a href="https://xerte.org.uk">xerte.org.uk</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	can
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	can

## Vendor Comments And Credit

### Discovery Credit

**CNA:** [bootstrapool \(en\)](#)

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)