Smart Slider 3 Pro 3.5.1.35 Supply Chain Attack Remote Access Toolkit

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

Summary

CVE	CVE-2026-34424
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 23:17:00 UTC
Updated	2026-04-09 23:17:00 UTC
Description	Smart Slider 3 Pro version 3.5.1.35 for WordPress and Joomla contains a multi-stage remote access toolkit injected throug

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

EPSS: 0.001520000 probability, percentile 0.359820000 (date 2026-04-10)

Problem Types: CWE-506 | CWE-506 CWE-506 Embedded Malicious Code

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

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	Nextendweb	Smart Slider 3 Pro For WordPress	affected 3.5.1.35 semver	Not specified
CNA	Nextendweb	Smart Slider 3 Pro For WordPress	unaffected 3.5.1.34 semver	Not specified
CNA	Nextendweb	Smart Slider 3 Pro For WordPress	unaffected 3.5.1.36 semver	Not specified

CNA	Nextendweb	Smart Slider 3 Pro For Joomla	affected 3.5.1.35 semver	Not specified
CNA	Nextendweb	Smart Slider 3 Pro For Joomla	unaffected 3.5.1.34 semver	Not specified
CNA	Nextendweb	Smart Slider 3 Pro For Joomla	unaffected 3.5.1.36 semver	Not specified

References

Reference	Source	Link
patchstack.com/database/wordpress/plugin/nextend-smart-slider3-pro/vulnerabi...	disclosure@vulncheck.com	patchstack.cor
smartslider.helpscoutdocs.com/article/2143-joomla-security-advisory-smart-slider-3-pro-3-5-...	disclosure@vulncheck.com	smartslider.he
mysites.guru/blog/smart-slider-3-pro-supply-chain-compromise	disclosure@vulncheck.com	mysites.guru
smartslider.helpscoutdocs.com/article/2144-wordpress-security-advisory-smart-slider-3-pro-3...	disclosure@vulncheck.com	smartslider.he
patchstack.com/articles/critical-supply-chain-compromise-in-smart-slider-3-p...	disclosure@vulncheck.com	patchstack.cor
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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