

CVE-2025-15556

Notepad++ Download of Code Without Integrity Check Vulnerability

CISA KEV since Feb 12, 2026

Actively exploited

Notepad++ versions prior to 8.8.9, when using the WinGUp updater, contain an update integrity verification vulnerability where downloaded update metadata and installers are not cryptographically verified. An attacker able to intercept or redirect update traffic can cause the updater to download and execute an attacker-controlled installer, resulting in arbitrary code execution with the privileges of the user.

EVRS 75/100 Urgent priority	CVSS V4.0 7.7 High · NVD	EPSS 0.018 78th percentile · FIRST	CISA DEADLINE Mar 5, 2026 CISA federal deadline · Overdue by 8 months
--	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.018 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.7	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
notepad\+\+	< 8.8.9	8.8.9	NVD

Sources

Vendor guidance	github.com/notepad-plus-plus/notepad-plus-plus/commit/bcf2aa68ef414338d717e20e059459570ed6c5ab	Additional guidance	notepad-plus-plus.org/news/hijacked-incident-info-update/
notepad-plus-plus.org	notepad-plus-plus.org/news/clarification-security-incident/	community.notepad-plus-plus.org	community.notepad-plus-plus.org/topic/27298/notepad-v8-8-9-vulnerability-fix
NVD	nvd.nist.gov/vuln/detail/CVE-2025-15556	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-206661	Current data	evulnable.com/vulnerability-management/cve/CVE-2025-15556

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.