Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2025-49144: A Silent Shortcut to SYSTEM Privileges in Notepad++

Date of Publication	Admiralty Code	TA Number
June 27, 2025	A1	TA2025201

Summary

Discovered On: June 2025
Affected Products: Notepad++
Impact: A newly disclosed vulnerability, CVE-2025-49144, affects the Notepad++ installer and could allow attackers to gain full control of a system. The flaw enables malicious actors to place a harmful file in the same directory as the installer, typically the 'Downloads' folder, which can be leveraged during installation to compromise the machine. This issue is slated to be addressed in Notepad++ version 8.8.2, and users are strongly advised to update once the fix is released to stay protected.

⚙ CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-49144	Notepad++ Privilege Escalation Vulnerability	Notepad++	❌	❌	❌

Vulnerability Details

#1

A high severity flaw has been discovered in the popular text editor Notepad++, which could allow attackers to gain full control over a Windows system. Tracked as CVE-2025-49144, this privilege escalation vulnerability affects the Notepad++ v8.8.1 installer and stems from insecure executable search paths. This means that under the right conditions, even users without admin rights can unknowingly trigger malicious code that executes with the highest level of system privileges.

#2 Notepad++ is widely used across the globe by developers, sysadmins, and general users for tasks ranging from code editing to scripting. The vulnerability puts millions at risk, as it can be exploited simply by placing a malicious executable in the same folder as the Notepad++ installer most commonly the default Downloads directory. This folder becomes a “vulnerable path,” where Windows might load the wrong file during installation, handing full system access to the attacker.

#3 The risk is amplified by the fact that proof-of-concept (PoC) code is now publicly available, making exploitation more accessible. An attacker could easily trick users through phishing, social engineering, or clickjacking into downloading both the legitimate Notepad++ installer and a crafted malicious file, such as a tampered version of a Windows utility like regsvr32.exe. Once the user runs the installer, the system automatically executes the rogue file with SYSTEM-level privileges, giving the attacker unrestricted control.

#4 To protect against this vulnerability, users should upgrade to Notepad++ version 8.8.2 as soon as it becomes available, as it addresses the issue. It's also good practice to avoid running installers directly from shared or default folders like 'Downloads' and to regularly clean up such directories to reduce exposure.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-49144	Notepad++ Versions 8.8.1 and prior	cpe:2.3:a:notepad-plus-plus:notepad:*:*:*:*:*:*:*	CWE-276 CWE-272 CWE-427

Recommendations

Update: If you're using Notepad++, make sure to update to version 8.8.2 as soon as it becomes available. This update addresses a vulnerability that could allow attackers to gain full control of your computer during installation.

Be Careful Where You Install From: Only download Notepad++ from the official website. Avoid third-party sources or links sent via email or social media.

Watch What's in Your Downloads Folder: Before running the installer, double-check your Downloads folder. Delete any suspicious or unknown files, especially executables (.exe) to prevent attackers from sneaking in malicious code.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation
T1204 User Execution	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1068** Exploitation for Privilege Escalation
T1566 Phishing			

Patch Details

Update your Notepad++ to version 8.8.2 as soon as it becomes available to address the vulnerability.

Link: https://notepad-plus-plus.org/downloads/

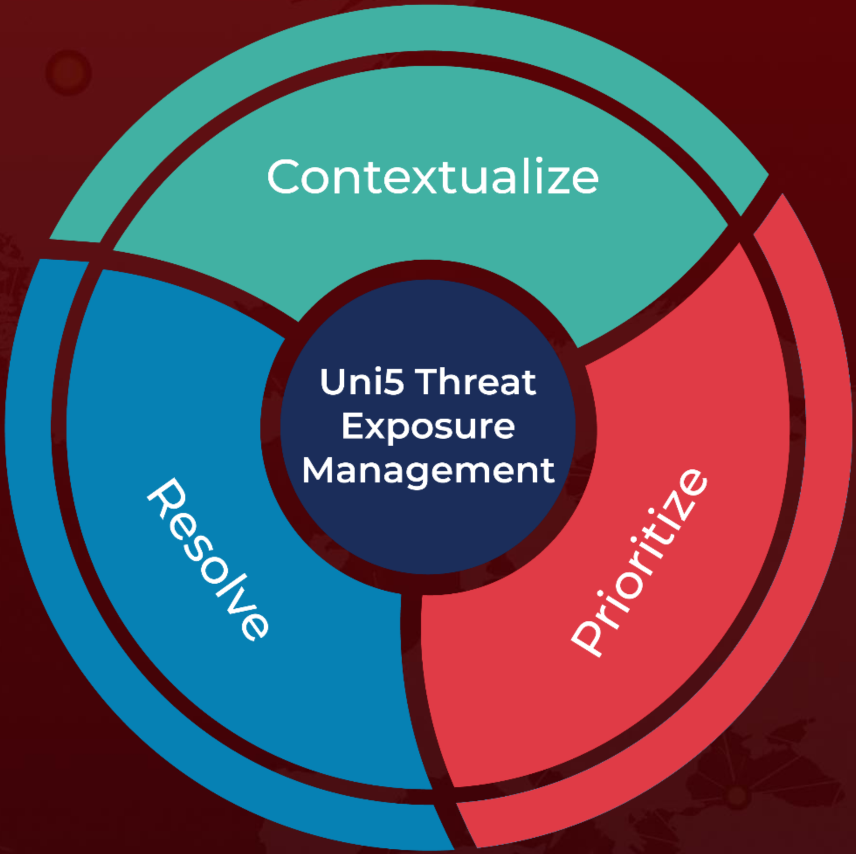
References

https://github.com/notepad-plus-plus/notepad-plus-plus/security/advisories/GHSA-9vx8-v79m-6m24

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 27, 2025 • 6:45 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com