Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Nuclei Vulnerability Exposes Systems to Malicious Code

Date of Publication	Admiralty Code	TA Number
January 6, 2025	A1	TA2025004

Summary

First Seen: August 14, 2024
Affected Products: ProjectDiscovery Nuclei
Impact: A significant security vulnerability has been uncovered in ProjectDiscovery's Nuclei, a popular open-source tool for vulnerability scanning. This severity flaw, identified as CVE-2024-43405, could enable attackers to bypass signature checks, potentially paving the way for the execution of malicious code.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-43405	ProjectDiscovery Nuclei Remote Code Execution Vulnerability	ProjectDiscovery Nuclei	✗	✗	✓

Vulnerability Details

#1

Nuclei, a powerful vulnerability scanner that leverages YAML-based templates, has been found to contain a high-severity flaw, tracked as CVE-2024-43405. This vulnerability affects Nuclei's template signature verification system and could allow attackers to bypass signature checks, enabling the execution of malicious code through custom templates.

#2 The issue arises from a mismatch in how the signer package processes signature verification and how the YAML parser handles newline characters. This discrepancy, coupled with the way multiple signatures are processed, enables an attacker to inject malicious content into a template while maintaining a valid signature for the benign portion of the template. Specifically, Nuclei processes only the first # digest: signature line in a template and ignores subsequent ones. An attacker could exploit this by appending additional malicious # digest: payloads containing harmful "code" sections, which bypass verification and are executed when the template is used.

#3 CLI users are particularly at risk if they execute custom templates from unverified sources, such as third-party authors or unofficial repositories. Similarly, SDK users integrating Nuclei into their platforms are affected if they allow the execution of custom code templates by end-users. The flaw also takes advantage of the way Go's regex-based signature verification interacts with YAML's line-break parsing, further complicating detection of malicious payloads.

#4 The vulnerability has been patched in Nuclei v3.3.2, and users are strongly urged to update to this version to mitigate the risk. A proof-of-concept (PoC) for this exploit is publicly available, further emphasizing the urgency of upgrading. As a temporary safeguard for users unable to update immediately, it is strongly recommended to avoid executing custom templates or to disable the feature entirely.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-43405	Nuclei prior to version 3.3.2	cpe:2.3:a:projectdiscovery:nuclei:*:*:*:*:*:go:*:*	CWE-78

Recommendations

Apply Patches: Immediately update to Nuclei v3.3.2 or a newer release, where the vulnerability has been patched. Delaying updates increases the risk of exploitation.

Restrict Custom Template Usage: Avoid using unverified or third-party custom code templates, especially from untrusted sources, until the update has been applied.

Run Nuclei in an Isolated Environment: Always deploy and execute Nuclei within a sandboxed or isolated environment to limit the potential impact of exploiting untrusted or community-contributed templates. This approach ensures that any malicious activity is contained, protecting critical systems and sensitive data.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	T1588 Obtain Capabilities	T1588.006 Vulnerabilities
T1059 Command and Scripting Interpreter			

Patch Details

Promptly update to Nuclei v3.3.2 or later, as this version includes the necessary patch to address the vulnerability.

Link: https://github.com/projectdiscovery/nuclei/releases

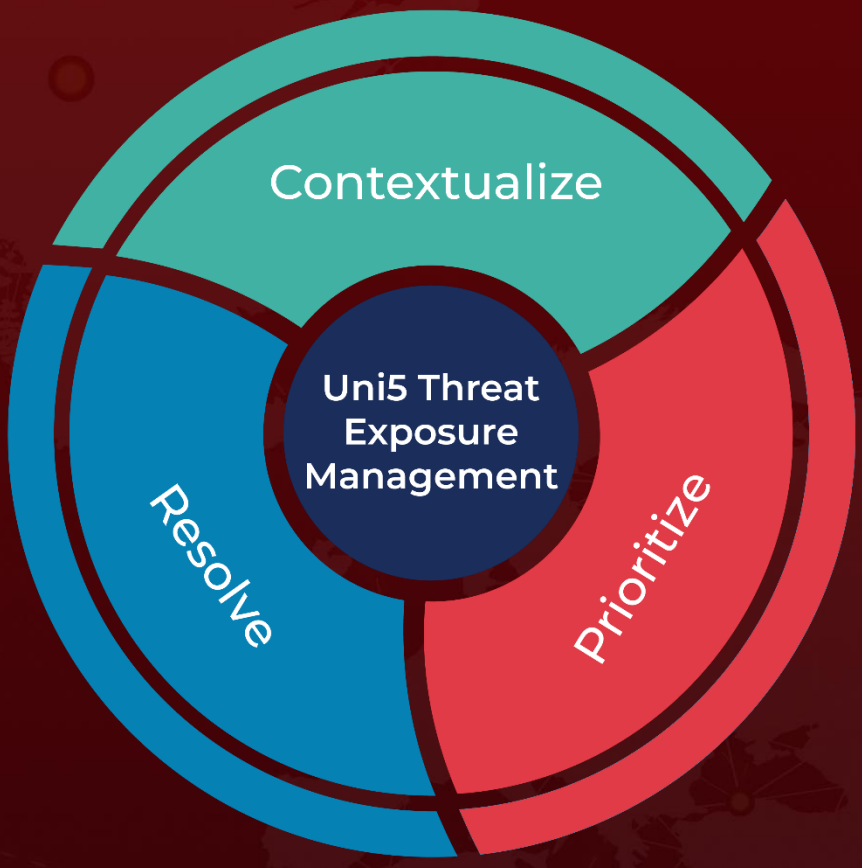
References

https://www.wiz.io/blog/nuclei-signature-verification-bypass

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

January 6, 2025 . 4:45 AM

More at www.hivepro.com