Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Flaw in SolarWinds Web Help Desk Leads to Remote Code Execution

Date of Publication	Admiralty Code	TA Number
August 16, 2024	A1	TA2024314

Summary

First Seen: August 2024
Affected Products: SolarWinds Web Help Desk
Impact: A critical vulnerability, designated as CVE-2024-28986, has been identified in SolarWinds' Web Help Desk, which could be exploited to achieve remote code execution. This flaw stems from a Java deserialization issue, potentially enabling an attacker to execute arbitrary commands on a vulnerable host machine.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-28986	SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability	SolarWinds Web Help Desk	✗	✓	✓

Vulnerability Details

#1 SolarWinds has released patches to address a critical vulnerability in its Web Help Desk (WHD) software, identified as CVE-2024-28986. This vulnerability, which carries a CVSS score of 9.8, is classified as a deserialization bug and could potentially allow attackers to execute arbitrary code on vulnerable systems.

#2 SolarWinds Web Help Desk (WHD) is a web-based IT service management (ITSM) solution widely used for managing and streamlining IT support, service delivery processes, tracking IT issues, handling service requests, and maintaining IT assets.

#3 This vulnerability stems from insecure input validation during the processing of serialized data. By exploiting this flaw, a remote attacker could pass specially crafted data to the application, resulting in the execution of arbitrary code on the affected system.

#4 Although CVE-2024-28986 was initially reported as a vulnerability that could be exploited without authentication, it has only been reproducible with authentication so far. Nonetheless, due to the critical nature of this flaw, it demands immediate attention and remediation.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-28986	SolarWinds Web Help Desk 12.8.3 and all previous versions	cpe:2.3:a:solarwinds:web_help_desk:*:*:*:*:*:*:*:*	CWE-502

Recommendations

Update: The vulnerability CVE-2024-28986 has been addressed in SolarWinds' Web Help Desk hotfix version 12.8.3 HF 1. Users are strongly encouraged to upgrade to this version to mitigate the risk of exploitation. It is recommended to create backup copies of the original files before applying the hotfix.

Implement Web Application Firewall (WAF): Deploy a WAF to monitor and filter incoming web traffic. A properly configured WAF can detect and block attempts to exploit the vulnerabilities, providing an additional layer of protection.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter	

Patch Details

All Web Help Desk users are strongly encouraged to apply the patch, which is now available in SolarWinds Web Help Desk version 12.8.3 HF 1.

Link: https://support.solarwinds.com/SuccessCenter/s/article/WHD-12-8-3-Hotfix-1

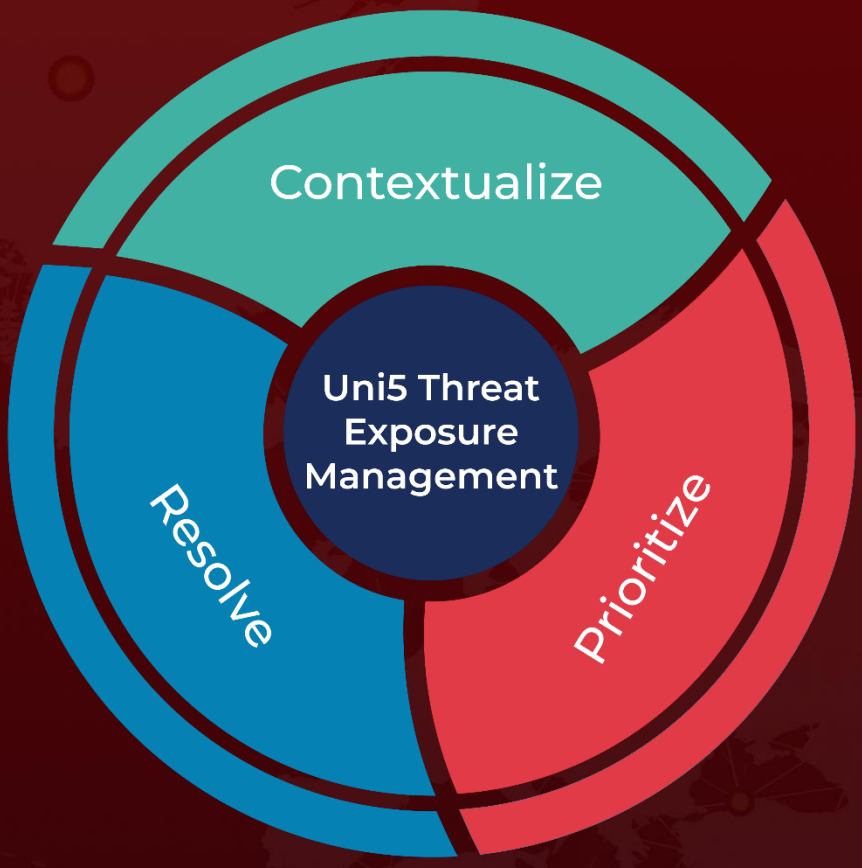
References

https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28986

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

August 16, 2024 • 5:30 AM

More at www.hivepro.com