Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

SolarWinds WHD Flaw Lets Attackers Infiltrate Systems with Hardcoded Credentials

Date of Publication	Admiralty Code	TA Number
August 23, 2024	A1	TA2024324

Summary

First Seen: August 2024
Affected Products: SolarWinds Web Help Desk (WHD)
Impact: SolarWinds has released a hotfix to address a critical vulnerability in its Web Help Desk software, identified as CVE-2024-28987. This flaw allows attackers to gain unauthorized access to unpatched systems using hardcoded credentials, potentially leading to unauthorized remote access and data modification.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-28987	SolarWinds Web Help Desk Hardcoded Credential Vulnerability	SolarWinds Web Help Desk (WHD)	✗	✓	✓

Vulnerability Details

#1 SolarWinds has released a hotfix to address a critical vulnerability in its Web Help Desk software, identified as CVE-2024-28987. This vulnerability allows attackers to gain unauthorized access to unpatched systems using hardcoded credentials, which could lead to unauthorized remote access and data modification.

#2 CVE-2024-28987 presents a significant security risk by potentially enabling malicious actors to log into vulnerable Web Help Desk instances, where they can access sensitive data and modify critical information without proper authorization.

#3 This disclosure follows shortly after SolarWinds released a patch for another critical vulnerability, CVE-2024-28986, in the same software, which could be exploited to execute arbitrary code. According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), CVE-2024-28986 has already been exploited in the wild.

#4 Administrators of SolarWinds Web Help Desk are strongly urged to apply the hotfix immediately to mitigate the risk of unauthorized access and protect their systems from potential threats. Prompt action will help ensure the security and integrity of their IT environments.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-28987	WHD 12.8.3 HF1 and all previous versions	cpe:2.3:a:solarwinds:web_help_desk:12.8.3_hotfix_1:*:*:*:*:*:*:*	CWE-798

Recommendations

Update: The vulnerability CVE-2024-28987 has been addressed in SolarWinds' Web Help Desk hotfix version 12.8.3 HF2. 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	TA0110 Persistence	TA0040 Impact
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	T1565 Data Manipulation
T0891 Hardcoded Credentials			

Patch Details

All users of SolarWinds Web Help Desk are strongly encouraged to apply the patch to address the critical vulnerability CVE-2024-28987. This patch is now available in SolarWinds Web Help Desk version 12.8.3 HF2.

Link:
https://support.solarwinds.com/SuccessCenter/s/article/SolarWinds-Web-Help-Desk-12-8-3-Hotfix-2

References

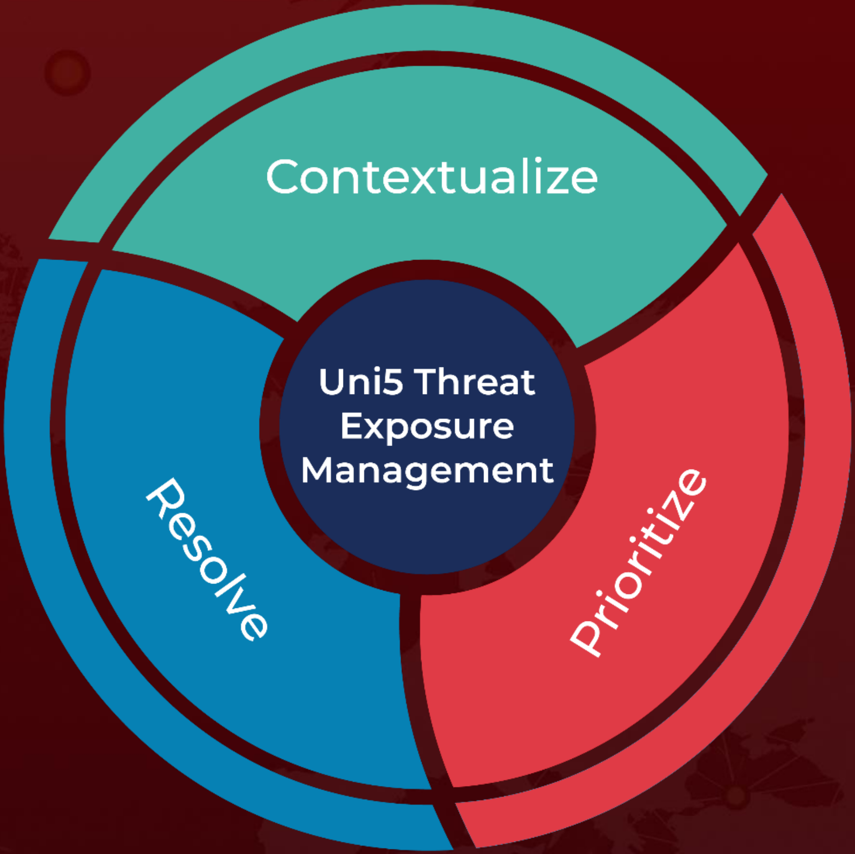
https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28987

https://hivepro.com/threat-advisory/critical-flaw-in-solarwinds-web-help-desk-leads-to-remote-code-execution/

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 23, 2024 • 6:10 AM

More at www.hivepro.com