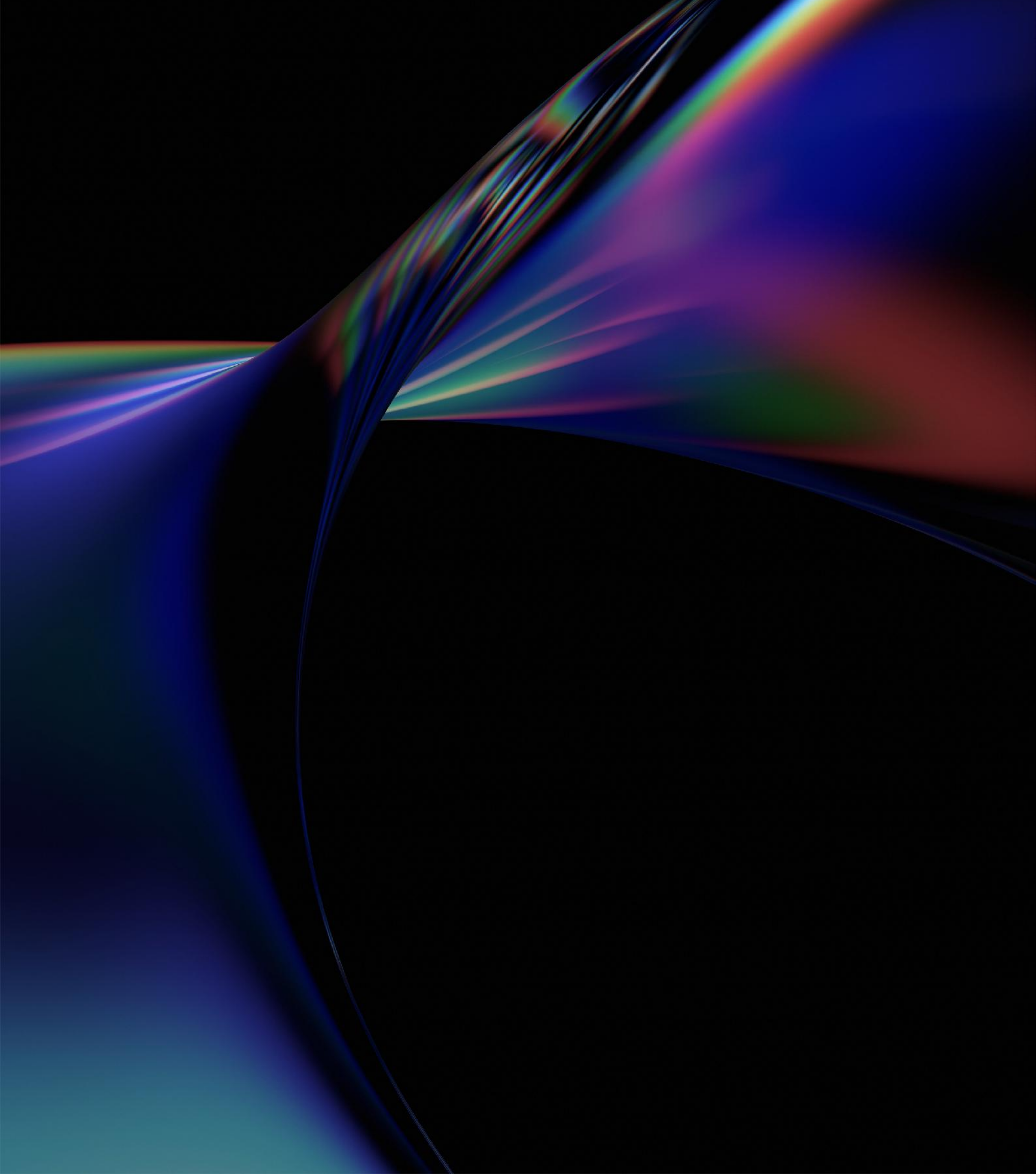
Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple Critical Vulnerabilities in SolarWinds Web Help Desk



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	14
Authors	Iana Denis Cristian < denis.iana@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-01-28
Issue Date	2026-01-28

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

Multiple vulnerabilities have been discovered in SolarWinds Web Help Desk, the most severe of which could allow for arbitrary code execution. SolarWinds Web Help Desk (WHD) is a web-based software that provides IT help desk and asset management functionality, allowing IT teams to manage service requests, track IT assets, and offer self-service options to end-users. Successful exploitation of the most severe of these vulnerabilities could allow an actor to execute code in the context of SYSTEM. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Risk

Government:

- Large and medium government entities: High
- Small government entities: High

Businesses:

- Large and medium business entities: High
- Small business entities: High

Technical summary

Critical vulnerabilities in SolarWinds Web Help Desk could allow remote code execution with SYSTEM-level privileges, leading to full compromise of the affected system. Details of the most severe vulnerabilities are as follows:

Tactic: Initial Access (TA0001):
Technique: Exploit Public-Facing Application (T1190):

Tactic: *Initial Access* (TA0001):
Technique: *Exploit Public-Facing Application* (T1190):

- SolarWinds Web Help Desk was found to be susceptible to an untrusted data deserialization vulnerability that could lead to unauthenticated remote code execution, if exploited, would allow an attacker to run commands on the host machine. (CVE-2025-40551 and CVE-2025-40553)
- SolarWinds Web Help Desk was found to be susceptible to an authentication bypass vulnerability that if exploited, would allow a malicious actor to execute actions and methods that should be protected by authentication. (CVE-2025-40552)
- SolarWinds Web Help Desk was found to be susceptible to an authentication bypass vulnerability, which if exploited, could allow an attacker to invoke specific actions within

Web Help Desk.(CVE-2025-40554)

- SolarWinds Web Help Desk was found to be susceptible to a security control bypass vulnerability that if exploited, could allow an unauthenticated attacker to gain access to certain restricted functionality. (CVE-2025-40536)
- SolarWinds Web Help Desk was found to be susceptible to a hardcoded credentials vulnerability that, under certain situations, could allow access to administrative functions. (CVE-2025-40537)

CVE-ID	Description
CVE-2025-40536 **CVSS Score: 8.1**	SolarWinds Web Help Desk was found to be susceptible to a security control bypass vulnerability that if exploited, could allow an unauthenticated attacker to gain access to certain restricted functionality.
CVE-2025-40537 **CVSS Score: 7.5**	SolarWinds Web Help Desk was found to be susceptible to a hardcoded credentials vulnerability that, under certain situations, could allow access to administrative functions.
CVE-2025-40551 **CVSS Score: 9.8**	SolarWinds Web Help Desk was found to be susceptible to an untrusted data deserialization vulnerability that could lead to remote code execution which would allow an attacker to run commands on the host machine. This could be exploited without authentication.
CVE-2025-40552 **CVSS Score: 9.8**	SolarWinds Web Help Desk was found to be susceptible to an authentication bypass vulnerability that if exploited, would allow a malicious actor to execute actions and methods that should be protected by authentication.
CVE-2025-40553 **CVSS Score: 9.8**	SolarWinds Web Help Desk was found to be susceptible to an untrusted data deserialization vulnerability that could lead to remote code execution which would allow an attacker to run commands on the host machine. This could be exploited without authentication.
CVE-2025-40554 **CVSS Score: 9.8**	SolarWinds Web Help Desk was found to be susceptible to an authentication bypass vulnerability, which if exploited, could allow an attacker to invoke specific actions within Web Help Desk.

Affected Versions:

Product Name	Affected Version(s)
SolarWinds Web Help Desk	versions prior to 2026.1

Recommendations

Smarttech247 team recommend the following actions to be taken:

Apply appropriate updates provided by SolarWinds or other vendors which use this software to vulnerable systems immediately after appropriate testing. (M1051: **Update Software**)

- **Safeguard 7.1 : Establish and Maintain a Vulnerability Management Process:** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
- **Safeguard 7.2: Establish and Maintain a Remediation Process:** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
- **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
- **Safeguard 7.5 : Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
- **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
- **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date:** Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
- **Safeguard 18.1: Establish and Maintain a Penetration Testing Program:** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
- **Safeguard 18.2: Perform Periodic External Penetration Tests:** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
- **Safeguard 18.3: Remediate Penetration Test Findings:** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.

Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (M1026: **Privileged Account Management**)

- **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
- **Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts:** Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them. (M1016: **Vulnerability Scanning**)

- **Safeguard 16.13: Conduct Application Penetration Testing:** Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems. (**M1030**: **Network Segmentation**)
Safeguard 12.2: Establish and Maintain a Secure Network Architecture: Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.

References

SolarWinds:

- https://documentation.solarwinds.com/en/success_center/whd/content/release_notes/whd_2026-1_release_notes.htm

CVE:

- CVE-2025-40536
  CVE-2025-40537
  CVE-2025-40551
  CVE-2025-40552
  CVE-2025-40553
  CVE-2025-40554

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com