

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

SolarWinds Critical ARM Flaw Exposing Systems to Remote Code Execution

Date of Publication

September 19, 2024

Admiralty Code

A1

TA Number

TA2024362




Summary

First Seen: September 12, 2024

Affected Products: SolarWinds Access Rights Manager (ARM)

Impact: SolarWinds has released a patch to address CVE-2024-28991, a critical vulnerability in its Access Rights Manager (ARM) software. This flaw could allow remote attackers to execute arbitrary code on affected systems, potentially leading to full system compromise. Users are strongly urged to apply the latest security updates to mitigate the risk of exploitation and ensure the continued protection of their environments.

CVE

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2024-28991	SolarWinds Access Rights Manager (ARM) Deserialization of Untrusted Data Remote Code Execution Vulnerability	SolarWinds Access Rights Manager (ARM)			

Vulnerability Details

#1

SolarWinds has addressed a critical security flaw, CVE-2024-28991, in its Access Rights Manager (ARM) software, which could potentially lead to remote code execution (RCE) and pose a severe risk to organizations. SolarWinds ARM is a key tool for IT and security administrators, streamlining the management, auditing, and control of user access rights to systems, data, and files.

#2

The CVE-2024-28991 vulnerability arises from improper data input handling within the `JsonSerializationBinder` class. Specifically, the system fails to adequately validate incoming data, allowing an attacker to inject malicious code that the application processes, resulting in the execution of harmful code with SYSTEM-level privileges. This gives the attacker full control over the compromised system.

#3

Although exploiting this vulnerability requires authentication, it's crucial to note that the existing authentication mechanism can be bypassed, potentially allowing unauthorized attackers to execute code on the system. To mitigate this risk, users are strongly advised to update to ARM version 2024.3.1 or later immediately.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-28991	SolarWinds ARM 2024.3 and prior versions	cpe:2.3:a:solarwinds:access_rights_manager:*:*:*:*:*:*:*	CWE-502

Recommendations



Update: Users are strongly urged to update SolarWinds Access Rights Manager (ARM) to version 2024.3.1 or later. This update is critical as it addresses the vulnerability associated with CVE-2024-28991, which could lead to remote code execution (RCE). Applying this update is essential to mitigate the risk and ensure the security of your systems.



Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks, restrict the access to the trusted parties only. This strategy reduces the effects of vulnerabilities related to privilege escalation.



Regularly Review: To maintain the security and integrity of your SolarWinds Access Rights Manager (ARM) system, it's crucial to implement a routine process for reviewing and auditing user permissions. This proactive measure helps ensure that only authorized personnel have the necessary access, reducing the risk of unauthorized access and potential security breaches.



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

<u>TA0042</u> Resource Development	<u>TA0002</u> Execution	<u>TA0004</u> Privilege Escalation	<u>TA0006</u> Credential Access
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1059</u> Command and Scripting Interpreter	<u>T1068</u> Exploitation for Privilege Escalation
<u>T1556</u> Modify Authentication Process			

Patch Details

Users are urged to update their systems as SolarWinds has addressed the vulnerability with the release of Access Rights Manager (ARM) version 2024.3.1.

Link:

https://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2024-3-1_release_notes.htm

References

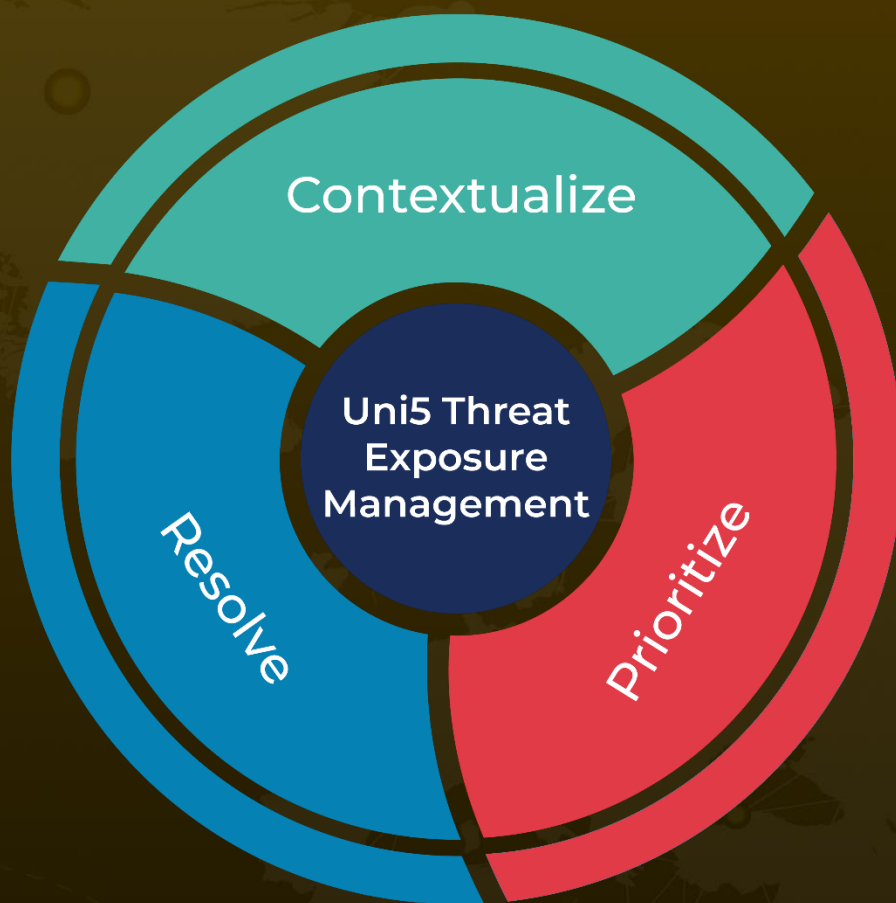
<https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28991>

<https://www.zerodayinitiative.com/advisories/ZDI-24-1224/>

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

September 19, 2024 • 6:00 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com