



NCSC-2024-0239

Kwetsbaarheden verholpen in Solarwinds Platform

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 07-06-2024

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Solarwinds heeft kwetsbaarheden verholpen in Solarwinds Platform.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om een Denial-of-Service te veroorzaken, een command-injection uit te voeren, of om een Cross-Site-Scripting-aanval uit te voeren. Een dergelijke aanval kan leiden tot uitvoer van willekeurige code in de browser van het slachtoffer.

Voor succesvol misbruik moet de kwaadwillende voorafgaande authenticatie hebben.

Oplossingen

Solarwinds heeft updates uitgebracht om de kwetsbaarheden te verhelpen in Solarwinds Platform 2024.2

In deze updates zijn tevens kwetsbaarheden verholpen in onderliggende third-party software waar het platform gebruik van maakt. Voor deze kwetsbaarheden zijn eerdere beveiligingsadviezen gepubliceerd.

Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://documentation.solarwinds.com/en/success_center/orionplatform/content/release_notes/solarwinds_platform_2024-2_release_notes.htm
- <https://www.solarwinds.com/trust-center/security-advisories/CVE-2024-28996>
- <https://www.solarwinds.com/trust-center/security-advisories/CVE-2024-28999>
- <https://www.solarwinds.com/trust-center/security-advisories/CVE-2024-29004>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2017-3736	
➤ CVE-2018-0732	
➤ CVE-2018-0737	
➤ CVE-2019-1559	

> CVE-2020-1971	
> CVE-2021-3712	
> CVE-2021-4321	
> CVE-2021-23840	
> CVE-2022-0778	
> CVE-2023-0215	
> CVE-2023-0286	
> CVE-2024-28996	8.1 HIGH
> CVE-2024-28999	8.1 HIGH
> CVE-2024-29004	7.1 HIGH

CWE's

CWE	Beschrijving
> CVE-125	Out-of-bounds Read
> CVE-190	Integer Overflow or Wraparound
> CVE-20	Improper Input Validation
> CVE-325	Missing Cryptographic Step
> CVE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
> CVE-385	Covert Timing Channel
> CVE-416	Use After Free
> CVE-476	NULL Pointer Dereference
> CVE-682	Incorrect Calculation
> CVE-704	Incorrect Type Conversion or Cast

> CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
> CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
> CWE-942	Permissive Cross-domain Policy with Untrusted Domains

Getroffen producten

solarwinds_
solarwinds_platform_
solarwinds_platform
solarwinds
orion_platform
solarwinds_platform_

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.