Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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