Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0421

Kwetsbaarheden verholpen in SolarWinds Serv-U

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 18-10-2024

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 Serv-U.

Duiding

Een kwaadwillende kan de kwetsbaarheid met kenmerk CVE-2024-45711 misbruiken om middels path-traversal willekeurige code uit te voeren op het onderliggende systeem. Voor succesvol misbruik moet de kwaadwillende voorafgaand geauthenticeerd zijn en code-uitvoer is mogelijk afhankelijk van de rechten van het account.

Ook kan de kwaadwillende de kwetsbaarheid met kenmerk CVE-2024-45714 misbruiken 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, of toegang tot gegevens in de context van de browser van het slachtoffer.

Het is aannemelijk dat de kwetsbaarheden in keten kunnen worden misbruikt. Door de aard van het systeem is daarmee niet uit te sluiten dat eventuele code-uitvoer via Cross-Site-Scripting met verhoogde rechten plaatsvindt. Omdat misbruik dan via social engineering plaats kan vinden, hoeft de kwaadwillende niet over voorafgaande authenticatie te beschikken, maar maakt de kwaadwillende misbruik van de rechten van het slachtoffer.

Oplossingen

SolarWinds heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.solarwinds.com/trust-center/security-advisories/CVE-2024-45711
- https://www.solarwinds.com/trust-center/security-advisories/CVE-2024-45714

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-45711	8.8 HIGH
CVE-2024-45714	4.8 MEDIUM

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Getroffen producten

solarwinds
serv- u
solarwinds_serv- u_managed_file_transfer_server__15.5

Disclaimer