Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0520

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in SolarWinds Serv-U

Publicatiedatum: 26-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

SolarWinds heeft meerdere kwetsbaarheden verholpen in Serv-U.

Duiding

De kwetsbaarheden in SolarWinds Serv-U betreffen verschillende aspecten van het product.

- Er is een ongeauthenticeerde HTTP response header injection die het mogelijk maakt om kwaadaardige inhoud in HTTP-headers te injecteren, wat kan leiden tot manipulatie van browser sessies.
- Daarnaast is er een command injection kwetsbaarheid op Windows-platforms waarbij onvoldoende validatie van gebruikersinvoer het uitvoeren van willekeurige commando's mogelijk maakt.
- Verder zijn er meerdere privilege escalatie kwetsbaarheden die het mogelijk maken voor gebruikers met domeinbeheerder- of hogere rechten om toegang te krijgen tot bestanden met hogere privileges, waaronder root-toegang op Linux-systemen.
- De authenticatieprocessen vertonen zwakheden door het ontbreken van effectieve brute-force bescherming, wat onbeperkte inlogpogingen mogelijk maakt, evenals een username enumeration flaw die het bestaan van gebruikersaccounts kan onthullen.
- Er is ook een out-of-bounds memory read kwetsbaarheid die het lezen van geheugen buiten de bedoelde grenzen toestaat.
- Een business logic kwetsbaarheid maakt het mogelijk voor gebruikers met hoge rechten en een geconfigureerde SMTP-server om commando's uit te voeren binnen de applicatiecontext.
- Daarnaast is er een denial-of-service kwetsbaarheid die bij bepaalde configuraties leidt tot overmatig geheugenverbruik en het weigeren van verbindingen.
- Meerdere Time-of-Check to Time-of-Use (TOCTOU) kwetsbaarheden stellen gebruikers met domeinbeheerderrechten in staat om beschermde bestanden buiten de bedoelde directorystructuur te benaderen of te wijzigen, wat kan resulteren in ongeautoriseerde code-uitvoering.
- Op Linux-platforms is er een stored cross-site scripting (XSS) kwetsbaarheid die het mogelijk maakt om kwaadaardige scripts uit te voeren binnen de administratieve sessie.
- Tenslotte zijn er type confusion kwetsbaarheden die privilege escalatie naar systeembeheerderniveau mogelijk maken, en een IDOR-kwetsbaarheid die domeingroepbeheerders toestaat om beperkingen te omzeilen en hun rechten te verhogen tot serverbeheerder.

De meeste van deze kwetsbaarheden vertonen een lager risico op Windows-platforms in vergelijking met andere omgevingen.

Oplossingen

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

Referenties

- https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_2026-4_release_notes.htm

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-123165	4.7 MEDIUM
CVE-2026-123166	7.2 HIGH
CVE-2026-123167	9.1 CRITICAL
CVE-2026-123168	9.1 CRITICAL
CVE-2026-123169	5.4 MEDIUM
CVE-2026-123170	6.5 MEDIUM
CVE-2026-123171	5.3 MEDIUM
CVE-2026-123172	9.1 CRITICAL
CVE-2026-123173	6.8 MEDIUM
CVE-2026-82313	8.4 HIGH
CVE-2026-82314	4.9 MEDIUM
CVE-2026-82315	9.1 CRITICAL
CVE-2026-82316	9.1 CRITICAL
CVE-2026-82317	6.8 MEDIUM
CVE-2026-82319	9.1 CRITICAL
CVE-2026-82320	9.1 CRITICAL
CVE-2026-82321	9.1 CRITICAL
CVE-2026-82322	9.1 CRITICAL

CWE's

CWE	Beschrijving
CWE-35	Path Traversal: '.../...//'
CWE-78	Improper Neutralization of Special Elements used in an OS Command
CWE-79	Improper Neutralization of Input During Web Page Generation
CWE-113	Improper Neutralization of CRLF Sequences in HTTP Headers
CWE-125	Out-of-bounds Read
CWE-203	Observable Discrepancy
CWE-250	Execution with Unnecessary Privileges
CWE-307	Improper Restriction of Excessive Authentication Attempts
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-843	Access of Resource Using Incompatible Type
CWE-862	Missing Authorization

Getroffen producten

SolarWinds
Serv-U

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.