Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0323

Kwetsbaarheden verholpen in Siemens Omnivise

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 06-08-2024

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

Siemens Energy heeft kwetsbaarheden verholpen in Omnivise T3000.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om zich verhoogde rechten toe te kennen op het kwetsbare systeem en daarmee willekeurige code uit te voeren, mogelijk met systeemrechten.

Voor succesvol misbruik moet de kwaadwillende lokaal geautoriseerd zijn. Echter, omdat de kwetsbaarheid met kenmerk CVE-2024-38879 een poort van een intern proces beschikbaar stelt op het netwerk, is het mogelijk dat de kwaadwillende op afstand de kwetsbaarheden in keten kan misbruiken. Hiervoor dient te kwaadwillende wel toegang te hebben tot de productie-omgeving. Het is goed gebruik een dergelijke omgeving niet publiek toegankelijk te hebben.

Oplossingen

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

Referenties

- https://cert-portal.siemens.com/productcert/html/ssa-857368.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-38876	7.8 HIGH
CVE-2024-38877	8.2 HIGH
CVE-2024-38878	7.2 HIGH
CVE-2024-38879	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-287	Improper Authentication
CWE-312	Cleartext Storage of Sensitive Information
CWE-552	Files or Directories Accessible to External Parties

Getroffen producten

siemens
omnivise_t3000_application_server
omnivise_t3000_domain_controller
omnivise_t3000_network_intrusion_detection_system__nids_
omnivise_t3000_network_intrusion_detection_system_nids_
omnivise_t3000_product_data_management__pdm_
omnivise_t3000_product_data_management_pdm_
omnivise_t3000_security_server
omnivise_t3000_terminal_server
omnivise_t3000_thin_client
omnivise_t3000_whitelisting_server

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.