



NCSC-2024-0355

Kwetsbaarheden verholpen in Progress WhatsUp Gold

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 02-09-2024

Revisie: 1.0.1

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

Update Revisie 1

Onderzoekers hebben Proof-of-Concept-code gepubliceerd.

Feiten

Progress heeft kwetsbaarheden verholpen in WhatsUp Gold.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om bij een Single User installatie het password van de applicatiegebruiker te achterhalen of wijzigen, of bij een Multi User installatie het password te wijzigen van een gebruiker met verhoogde rechten middels een SQL-Injection. Hiermee kan de kwaadwillende toegang tot de applicatie krijgen met verhoogde rechten.

Onderzoekers hebben Proof-of-Concept-code (PoC) gepubliceerd, waarmee de kwetsbaarheid met kenmerk CVE-2024-6670 kan worden aangetoond. Misbruik vereist een single-user installatie en dat de kwaadwillende toegang heeft tot de interface van het systeem. Het is goed gebruik een dergelijke beheer- en monitoring-tool als WhatsUp niet publiek toegankelijk te hebben, maar af te steunen op een separate beheeromgeving.

Oplossingen

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

Referenties

➤ <https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-August-2024>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-6670	9.8 CRITICAL
➤ CVE-2024-6671	9.8 CRITICAL
➤ CVE-2024-6672	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Getroffen producten

progress_software_corporation
whatsup_gold

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.