



NCSC-2024-0268

Kwetsbaarheden verholpen in Progress WhatsUp Gold

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 08-08-2024

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

Er is Proof-of-Concept-code (PoC) gepubliceerd die de kwetsbaarheid met kenmerk CVE-2024-4885 aantoont.

Feiten

Progress heeft kwetsbaarheden verholpen in WhatsUp Gold.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om een Denial-of-Service te veroorzaken, of willekeurige code uit te voeren, mogelijk met rechten van het systeem. Door diverse kwetsbaarheden in keten te misbruiken kan het daarmee voor de kwaadwillende mogelijk worden het systeem waarop WhatsUp Gold is geïnstalleerd over te nemen.

Voor de kwetsbaarheid met kenmerk CVE-2024-4885 is Proof-of-Concept-code (PoC) verschenen. Deze kwetsbaarheid maakt het mogelijk om code uit te voeren met rechten van het proces iisappool\nmconsole. Succesvol misbruik vereist dat de kwaadwillende toegang heeft tot de omgeving waarin WhatsUp Gold is geïmplementeerd.

Oplossingen

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

Referenties

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

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-4883	9.8 CRITICAL
➤ CVE-2024-4884	9.8 CRITICAL
➤ CVE-2024-4885	9.8 CRITICAL
➤ CVE-2024-5008	8.8 HIGH

> CVE-2024-5009	8.4 HIGH
> CVE-2024-5010	7.5 HIGH
> CVE-2024-5011	7.5 HIGH
> CVE-2024-5012	8.6 HIGH
> CVE-2024-5013	7.5 HIGH
> CVE-2024-5014	7.1 HIGH
> CVE-2024-5015	7.1 HIGH
> CVE-2024-5016	7.2 HIGH
> CVE-2024-5017	6.5 MEDIUM
> CVE-2024-5018	5.3 MEDIUM
> CVE-2024-5019	5.3 MEDIUM

CWE's

CWE	Beschrijving
> CVE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CVE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CVE-269	Improper Privilege Management
> CVE-287	Improper Authentication
> CVE-400	Uncontrolled Resource Consumption
> CVE-434	Unrestricted Upload of File with Dangerous Type
> CVE-502	Deserialization of Untrusted Data
> CVE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
> CVE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

➤ CWE-918	Server-Side Request Forgery (SSRF)
➤ CWE-94	Improper Control of Generation of Code ('Code 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.