Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0268

Kwetsbaarheden verholpen in Progress WhatsUp Gold

2024-08-08 Revisie 1

Updates

Revision: 0

Initiele versie

Revision: 1

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

Toegestande verspreiding: 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.firs t.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Progress heeft kwetsbaarheden verholpen in WhatsUp Gold.

Interpretaties

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 iisapppool\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