Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0234

Kwetsbaarheid verholpen in Github Enterprise Server

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 23-05-2024

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

Github heeft een kwetsbaarheid verholpen in Github Enterprise Server.

Duiding

Een kwaadwillende kan de kwetsbaarheid misbruiken om toegang te krijgen tot de Github-omgeving, mogelijk zelfs als administrator.

De kwetsbaarheid bevindt zich in de wijze waarop Github SAML-Single-Sign-on verwerkt. Wanneer gebruik wordt gemaakt van de optionele 'Security Assertions' kan de kwaadwillende zonder voorafgaande authenticatie toegang krijgen tot willekeurige accounts, waaronder die van beheerders.

SAML-SSO is standaard niet in gebruik. 'Security Assertions' zijn optioneel en standaard niet geconfigureerd. Bij reguliere installaties, die beide configuratie-opties niet in gebruik hebben, is misbruik niet mogelijk.

Oplossingen

Github heeft updates beschikbaar gesteld om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie:

https://docs.github.com/en/enterprise-server@3.10/admin/release-notes#3.10.12

https://docs.github.com/en/enterprise-server@3.11/admin/release-notes#3.11.10

https://docs.github.com/en/enterprise-server@3.12/admin/release-notes#3.12.4

https://docs.github.com/en/enterprise-server@3.9/admin/release-notes#3.9.15

Referenties

- https://docs.github.com/en/enterprise-server@3.10/admin/release-notes#3.10.12
- https://docs.github.com/en/enterprise-server@3.11/admin/release-notes#3.11.10
- https://docs.github.com/en/enterprise-server@3.12/admin/release-notes#3.12.4
- https://docs.github.com/en/enterprise-server@3.9/admin/release-notes#3.9.15

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-4985	

CWE's

CWE	Beschrijving
CWE-303	Incorrect Implementation of Authentication Algorithm

Getroffen producten

github
enterprise_server

Disclaimer