Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0316

Kwetsbaarheid verholpen in Broadcom Symantec Privileged Access Management

2024-07-22 Revisie 0

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

Broadcom heeft kwetsbaarheden verholpen in Broadcom Symantec Privileged Access Management.

Interpretaties

Een kwaadwillende kan de kwetsbaarheden misbruiken om willekeurige code uit te voeren op het systeem of om de werking van het systeem te manipuleren.

De kwetsbaarheden met kenmerken CVE-2024-36455, CVE-2024-36456 en CVE-2024-38492 stellen een ongeauthenticeerde kwaadwillende in staat om willekeurige code uit te voeren in de scope van een geauthenticeerd slachtoffer. Succesvol misbruik vereist wel dat de kwaadwillende toegang heeft tot de infrastructuur waar Broadcom Symantec Privileged Access Management op draait. Het is goed gebruik een dergelijke interface niet publiek toegankelijk te hebben.

Oplossingen

Broadcom heeft updates uitgebracht om de kwetsbaarheden in Broadcom Symantec Privileged Access Management te verhelpen. Zie bijgevoegde referenties voor meer informatie. Om de security advisory in te zien moet worden ingelogd met een Broadcom account.

Referenties

- https://nvd.nist.gov/vuln/detail/CVE-2024-36455
- https://nvd.nist.gov/vuln/detail/CVE-2024-36456
- https://nvd.nist.gov/vuln/detail/CVE-2024-36457
- https://nvd.nist.gov/vuln/detail/CVE-2024-36458
- https://nvd.nist.gov/vuln/detail/CVE-2024-38492
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24678