



Advisory NCSC-2024-0440

Kwetsbaarheden verholpen in Citrix Session Recording

2024-11-13 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.first.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

Citrix heeft kwetsbaarheden verholpen in Citrix Session Recording

Interpretaties

Een kwaadwillende met beperkte rechten kan de kwetsbaarheden misbruiken om toegang te verkrijgen tot service accounts en willekeurige code uit te voeren op de server.

Onderzoekers hebben Proof-of-Concept-code gepubliceerd, waarmee de kwetsbaarheid met kenmerk CVE-2024-8069 kan worden aangetoond. Het is goed gebruik een dergelijke interface niet publiek toegankelijk te hebben, maar af te steunen in een separate beheeromgeving.

Oplossingen

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

Referenties

- <https://www.cve.org/CVERecord?id=CVE-2024-8068>
- <https://www.cve.org/CVERecord?id=CVE-2024-8069>
- <https://support.citrix.com/s/article/CTX691941-citrix-session-recording-security-bulletin-for-cve20248068-and-cve20248069>