Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0384

Kwetsbaarheden ontdekt in CUPS

2024-10-02 Revisie 1

Updates

Revision: 0

Initiele versie

Revision: 1

New revision

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

Onlangs zijn er door een onderzoeker een aantal kwetsbaarheden ontdekt in CUPS die kunnen leiden tot Remote Code Execution. Deze zijn bekend gemaakt als "9.9 RCE affecting all GNU/Unix systems".

Interpretaties

Door een aaneenschakeling van de vier kwetsbaarheden, kan een kwaadwillende onder bepaalde omstandigheden willekeurige code uitvoeren binnen de context van de CUPS-service.

Oplossingen

Er zijn op dit moment nog geen patches beschikbaar om de kwetsbaarheden te verhelpen in CUPS versies lager dan 2.0.1.

Tot het moment dat de updates beschikbaar komen is het handelingsperspectief om de cups-browse daemon uit te schakelen.

Tevens is het raadzaam om te controleren of CUPS onbereikbaar is vanaf publieke netwerken. Controleer of verkeer van en naar UDP poort 631 wordt geblokkeerd. Hiermee wordt het risico van misbruik vanaf publieke netwerken verminderd.

UPDATE Er zijn patches beschikbaar gesteld om de kwetsbaarheden te verhelpen. Deze zijn doorgevoerd in de distributies van GNU/Linux systemen.

Referenties

- https://nvd.nist.gov/vuln/detail/CVE-2024-47076
- https://nvd.nist.gov/vuln/detail/CVE-2024-47175
- https://nvd.nist.gov/vuln/detail/CVE-2024-47176
- https://nvd.nist.gov/vuln/detail/CVE-2024-47177