



NCSC-2024-0384

Kwetsbaarheden ontdekt in CUPS

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 27-09-2024

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

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".

Duiding

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 UPS poort 631 wordt geblokkeerd. Hiermee wordt het risico van misbruik vanaf publieke netwerken verminderd.

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>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-47175	
➤ CVE-2024-47176	8.3 HIGH
➤ CVE-2024-47177	9.0 CRITICAL
➤ CVE-2024-47076	8.6 HIGH

CWE's

CWE	Beschrijving
➤ CWE-1327	Binding to an Unrestricted IP Address
➤ CWE-940	Improper Verification of Source of a Communication Channel
➤ CWE-749	Exposed Dangerous Method or Function
➤ CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
➤ CWE-20	Improper Input Validation

Getroffen producten

openprinting
cups-browsed
cups-filters
libcupsfilters

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.