Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0015

Kwetsbaarheden verholpen in Rsync

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 15-01-2025

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

Rsync Project heeft kwetsbaarheden verholpen in Rsync (versies <3.4.0).

Duiding

De meest kritieke kwetsbaarheden in Rsync omvatten een heap-gebaseerde 'buffer overflow' (CVE-2024-12084) en een 'info leak' (CVE-2024-12085) die kunnen leiden tot willekeurige code-executie (aanwezig in Rsync-versies 3.2.7 & 3.3.0). Daarnaast zijn er kwetsbaarheden gerelateerd aan 'path traversal' en onjuiste verificatie van symbolische links, wat kan leiden tot ongeautoriseerde toegang tot gevoelige gegevens en het schrijven van bestanden buiten de bedoelde directory. Deze kwetsbaarheden kunnen worden misbruikt door aanvallers om de beschikbaarheid, integriteit en vertrouwelijkheid in gevaar te brengen.

Gezien de bekendheid van Rsync en de brede implementatie verwacht het NCSC op korte termijn PoC code.

Oplossingen

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

Referenties

- https://www.kb.cert.org/vuls/id/952657
- https://rsync.samba.org/ftp/rsync/NEWS.html#3.4.0
- https://github.com/RsyncProject/rsync/releases/tag/v3.4.0

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-12084	
CVE-2024-12085	
CVE-2024-12086	
CVE-2024-12087	
CVE-2024-12088	
CVE-2024-12747	

CWE's

CWE	Beschrijving
CWE-457	Use of Uninitialized Variable
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-122	Heap-based Buffer Overflow
CWE-390	Detection of Error Condition Without Action
CWE-35	Path Traversal: '.../...//'
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Disclaimer