Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0290

Kwetsbaarheden verholpen in Juniper Junos OS en Junos OS Evolved

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 12-07-2024

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

Er zijn kwetsbaarheden gevonden en verholpen in Juniper Junos OS en Junos OS Evolved.

Duiding

De kwetsbaarheden stellen een kwaadwillende in staat aanvallen uit te voeren die kunnen leiden tot Denial-of-Service (DoS), toegang tot gevoelige informatie, uitvoeren van code met verhoogde gebruikersrechten en omzeilen van een beveiligingsmaatregel.

Oplossingen

Juniper heeft updates uitgebracht om de kwetsbaarheden te verhelpen in JunOS en JunOS Evolved. Zie de referenties voor meer informatie.

Referenties

- https://api.first.org/data/v1/epss?cve=CVE-2024-39511
- https://api.first.org/data/v1/epss?cve=CVE-2024-39514
- https://api.first.org/data/v1/epss?cve=CVE-2024-39517
- https://api.first.org/data/v1/epss?cve=CVE-2024-39518
- https://api.first.org/data/v1/epss?cve=CVE-2024-39554
- https://api.first.org/data/v1/epss?cve=CVE-2024-39555
- https://api.first.org/data/v1/epss?cve=CVE-2024-39556
- https://api.first.org/data/v1/epss?cve=CVE-2024-39558
- https://api.first.org/data/v1/epss?cve=CVE-2024-39560
- https://api.first.org/data/v1/epss?cve=CVE-2024-39561
- https://nvd.nist.gov/vuln/detail/CVE-2024-39511
- https://nvd.nist.gov/vuln/detail/CVE-2024-39514
- https://nvd.nist.gov/vuln/detail/CVE-2024-39517
- https://nvd.nist.gov/vuln/detail/CVE-2024-39518
- https://nvd.nist.gov/vuln/detail/CVE-2024-39528
- https://nvd.nist.gov/vuln/detail/CVE-2024-39530
- https://nvd.nist.gov/vuln/detail/CVE-2024-39532
- https://nvd.nist.gov/vuln/detail/CVE-2024-39533
- https://nvd.nist.gov/vuln/detail/CVE-2024-39536
- https://nvd.nist.gov/vuln/detail/CVE-2024-39539
- https://nvd.nist.gov/vuln/detail/CVE-2024-39540
- https://nvd.nist.gov/vuln/detail/CVE-2024-39541
- https://nvd.nist.gov/vuln/detail/CVE-2024-39542

- https://nvd.nist.gov/vuln/detail/CVE-2024-39543
- https://nvd.nist.gov/vuln/detail/CVE-2024-39545
- https://nvd.nist.gov/vuln/detail/CVE-2024-39549
- https://nvd.nist.gov/vuln/detail/CVE-2024-39550
- https://nvd.nist.gov/vuln/detail/CVE-2024-39551
- https://nvd.nist.gov/vuln/detail/CVE-2024-39552
- https://nvd.nist.gov/vuln/detail/CVE-2024-39554
- https://nvd.nist.gov/vuln/detail/CVE-2024-39555
- https://nvd.nist.gov/vuln/detail/CVE-2024-39556
- https://nvd.nist.gov/vuln/detail/CVE-2024-39558
- https://nvd.nist.gov/vuln/detail/CVE-2024-39560
- https://nvd.nist.gov/vuln/detail/CVE-2024-39561
- https://www.cve.org/CVERecord?id=CVE-2024-39511
- https://www.cve.org/CVERecord?id=CVE-2024-39514
- https://www.cve.org/CVERecord?id=CVE-2024-39517
- https://www.cve.org/CVERecord?id=CVE-2024-39518
- https://www.cve.org/CVERecord?id=CVE-2024-39528
- https://www.cve.org/CVERecord?id=CVE-2024-39530
- https://www.cve.org/CVERecord?id=CVE-2024-39532
- https://www.cve.org/CVERecord?id=CVE-2024-39533
- https://www.cve.org/CVERecord?id=CVE-2024-39536
- https://www.cve.org/CVERecord?id=CVE-2024-39539
- https://www.cve.org/CVERecord?id=CVE-2024-39540
- https://www.cve.org/CVERecord?id=CVE-2024-39541
- https://www.cve.org/CVERecord?id=CVE-2024-39542
- https://www.cve.org/CVERecord?id=CVE-2024-39543
- https://www.cve.org/CVERecord?id=CVE-2024-39545
- https://www.cve.org/CVERecord?id=CVE-2024-39549
- https://www.cve.org/CVERecord?id=CVE-2024-39550
- https://www.cve.org/CVERecord?id=CVE-2024-39551
- https://www.cve.org/CVERecord?id=CVE-2024-39552
- https://www.cve.org/CVERecord?id=CVE-2024-39554
- https://www.cve.org/CVERecord?id=CVE-2024-39555
- https://www.cve.org/CVERecord?id=CVE-2024-39556
- https://www.cve.org/CVERecord?id=CVE-2024-39558
- https://www.cve.org/CVERecord?id=CVE-2024-39560
- https://www.cve.org/CVERecord?id=CVE-2024-39561
- https://supportportal.juniper.net/JSA75726
- https://supportportal.juniper.net/JSA79175
- https://supportportal.juniper.net/JSA82976
- https://supportportal.juniper.net/JSA82980

- https://supportportal.juniper.net/JSA82982
- https://supportportal.juniper.net/JSA82987
- https://supportportal.juniper.net/JSA82989
- https://supportportal.juniper.net/JSA82992
- https://supportportal.juniper.net/JSA82993
- https://supportportal.juniper.net/JSA82996
- https://supportportal.juniper.net/JSA82999
- https://supportportal.juniper.net/JSA83000
- https://supportportal.juniper.net/JSA83001
- https://supportportal.juniper.net/JSA83002
- https://supportportal.juniper.net/JSA83004
- https://supportportal.juniper.net/JSA83007
- https://supportportal.juniper.net/JSA83011
- https://supportportal.juniper.net/JSA83012
- https://supportportal.juniper.net/JSA83013
- https://supportportal.juniper.net/JSA83014
- https://supportportal.juniper.net/JSA83015
- https://supportportal.juniper.net/JSA83016
- https://supportportal.juniper.net/JSA83018
- https://supportportal.juniper.net/JSA83020
- https://supportportal.juniper.net/JSA83021
- https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-39560	6.5 MEDIUM
CVE-2024-39561	5.8 MEDIUM
CVE-2024-39511	5.5 MEDIUM
CVE-2024-39514	6.5 MEDIUM
CVE-2024-39517	6.5 MEDIUM
CVE-2024-39518	7.5 HIGH
CVE-2024-39528	5.7 MEDIUM

CVE-2024-39530	7.5 HIGH
CVE-2024-39532	6.3 MEDIUM
CVE-2024-39533	5.8 MEDIUM
CVE-2024-39536	5.3 MEDIUM
CVE-2024-39539	5.3 MEDIUM
CVE-2024-39540	7.5 HIGH
CVE-2024-39541	6.5 MEDIUM
CVE-2024-39542	7.5 HIGH
CVE-2024-39543	6.5 MEDIUM
CVE-2024-39545	7.5 HIGH
CVE-2024-39549	7.5 HIGH
CVE-2024-39550	6.5 MEDIUM
CVE-2024-39551	7.5 HIGH
CVE-2024-39552	7.5 HIGH
CVE-2024-39554	5.9 MEDIUM
CVE-2024-39555	7.5 HIGH
CVE-2024-39556	
CVE-2024-39558	6.5 MEDIUM

CWE's

CWE	Beschrijving
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-121	Stack-based Buffer Overflow

CWE-122	Heap-based Buffer Overflow
CWE-20	Improper Input Validation
CWE-252	Unchecked Return Value
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-400	Uncontrolled Resource Consumption
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-404	Improper Resource Shutdown or Release
CWE-416	Use After Free
CWE-447	Unimplemented or Unsupported Feature in UI
CWE-532	Insertion of Sensitive Information into Log File
CWE-703	Improper Check or Handling of Exceptional Conditions
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-755	Improper Handling of Exceptional Conditions

Getroffen producten

juniper_networks
junos_os_evolved
junos_os
juniper
junos_os_evolved
junos
junos_os

Disclaimer