DJ-CERT
Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 11-10-2024

BULLETIN ALERTES

Object	Multiples vulnérabilités affectant plusieurs produits de Juniper
Réference	1259
Date de Publication	2024-10-11
Sévérité	Elevé

IMPACT :

- Déni de service
- Exécution de code arbitraire
- Elévation de privilèges
- Accès à des données confidentielles
- Contournement de mesures de sécurité

SYSTÉME AFFECTÉ :

- Plusieurs versions de Junos OS Evolved. Veuillez se référer aux bulletins de sécurité de l'éditeur pour trouver les versions vulnérables
- Junos Space versions antérieures à 24.1R1 Patch v2
- Plusieurs versions de Junos OS. Veuillez se référer aux bulletins de sécurité de l'éditeur pour trouver les versions vulnérables

DÉSCRIPTION :

Plusieurs vulnérabilités ont été découvertes affectant plusieurs versions de ses produits susmentionnés. Un attaquant distant pourrait exploiter ces vulnérabilités pour exécuter du code arbitraire, élever ses privilèges, contourner des mesures de sécurité, accéder à des données confidentielles ou causer un déni de service.

SOLUTION :

Veuillez se référer aux bulletins de sécurité de Juniper afin d'installer les nouvelles mises à jour.

DOCUMENTATION :

- Bulletins de sécurité juniper:

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-Due-to-a-race-condition-AgentD-process-causes-a-memory-corruption-and-FPC-reset-CVE-2024-47494

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-Evolved-ACX-7000-Series-Receipt-of-specific-transit-MPLS-packets-causes-resources-to-be-exhausted-CVE-2024-47490

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-Evolved-ACX-Series-Receipt-of-specific-transit-protocol-packets-is-incorrectly-processed-by-the-RE-CVE-2024-47489

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-Evolved-Connections-to-the-network-and-broadcast-address-accepted-CVE-2024-39534

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-Evolved-In-a-dual-RE-scenario-a-locally-authenticated-attacker-with-shell-privileges-can-take-over-the-device-CVE-2024-47495

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-Evolved-Low-privileged-local-user-able-to-view-NETCONF-traceoptions-files-CVE-2024-39544

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-Evolved-Multiple-vulnerabilities-resolved-in-c-ares-1-18-1

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-Evolved-QFX5000-Series-Configured-MAC-learning-and-move-limits-are-not-in-effect-CVE-2024-47498

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-Evolved-Specific-low-privileged-CLI-commands-and-SNMP-GET-requests-can-trigger-a-resource-leak

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-Evolved-TCP-session-state-is-not-always-cleared-on-the-Routing-Engine-CVE-2024-47502

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-J-Web-Multiple-vulnerabilities-resolved-in-PHP-software

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-MX-Series-The-PFE-will-crash-on-running-specific-command-CVE-2024-47496

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-MX304-MX-with-MPC10-11-LC9600-and-EX9200-with-EX9200-15C-In-a-VPLS-or-Junos-Fusion-scenario-specific-show-commands-cause-an-FPC-crash-CVE-2024-47501

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-Multiple-vulnerabilities-in-OSS-component-nginx-resolved

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-Multiple-vulnerabilities-resolved-in-OpenSSL

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-SRX-Series-A-large-amount-of-traffic-being-processed-by-ATP-Cloud-can-lead-to-a-PFE-crash-CVE-2024-47506

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-SRX-S

eries-Low-privileged-user-able-to-access-sensitive-information-on-file-system-CVE-2024-39527

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-SRX-Series-QFX-Series-MX-Series-and-EX-Series-Receiving-specific-HTTPS-traffic-causes-resource-exhaustion-CVE-2024-47497

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-SRX4600-and-SRX5000-Series-Sequence-of-specific-PIM-packets-causes-a-flowd-crash-CVE-2024-47503

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-SRX5000-Series-Receipt-of-a-specific-malformed-packet-will-cause-a-flowd-crash-CVE-2024-47504

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-SRX5K-SRX4600-and-MX-Series-Trio-based-FPCs-Continuous-physical-interface-flaps-causes-local-FPC-to-crash-CVE-2024-47493

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-BGP-update-message-containing-aggregator-attribute-with-an-ASN-value-of-zero-0-is-accepted-CVE-2024-47507

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-In-a-BMP-scenario-receipt-of-a-malformed-AS-PATH-attribute-can-cause-an-RPD-core-CVE-2024-47499

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Junos-OS-and-Junos-OS-Evolved-Receipt-of-a-specifically-malformed-BGP-packet-causes-RPD-crash-when-segment-routing-is-enabled-CVE-2024-39516

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-MX-Series-with-MPC10-MPC11-LC9600-MX304-EX9200-PTX-Seri

es-Receipt-of-malformed-DHCP-packets-causes-interfaces-to-stop-processing-packets-CVE-2024-39526

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Receipt-of-a-specific-malformed-BGP-path-attribute-leads-to-an-RPD-crash-CVE-2024-47491

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-When-BGP-nexthop-traceoptions-is-enabled-receipt-of-specially-crafted-BGP-packet-causes-RPD-crash-CVE-2024-39525

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-With-BGP-traceoptions-enabled-receipt-of-specially-crafted-BGP-update-causes-RPD-crash-CVE-2024-39515

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-cRPD-Receipt-of-crafted-TCP-traffic-can-trigger-high-CPU-utilization-CVE-2024-39547

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-Space-OS-command-injection-vulnerability-in-OpenSSH-CVE-2023-51385

https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-Space-Remote-Command-Execution-RCE-vulnerability-in-web-application-CVE-2024-39563

- CVE-2016-0742

https://www.cve.org/CVERecord?id=CVE-2016-0742

- CVE-2016-0746

https://www.cve.org/CVERecord?id=CVE-2016-0746

- CVE-2016-0747

https://www.cve.org/CVERecord?id=CVE-2016-0747

- CVE-2016-1247

https://www.cve.org/CVERecord?id=CVE-2016-1247

- CVE-2016-4450

https://www.cve.org/CVERecord?id=CVE-2016-4450

- CVE-2017-20005

https://www.cve.org/CVERecord?id=CVE-2017-20005

- CVE-2017-7529

https://www.cve.org/CVERecord?id=CVE-2017-7529

- CVE-2018-16845

https://www.cve.org/CVERecord?id=CVE-2018-16845

- CVE-2019-20372

https://www.cve.org/CVERecord?id=CVE-2019-20372

- CVE-2021-23017

https://www.cve.org/CVERecord?id=CVE-2021-23017

- CVE-2021-3618

https://www.cve.org/CVERecord?id=CVE-2021-3618

- CVE-2022-41741

https://www.cve.org/CVERecord?id=CVE-2022-41741

- CVE-2022-41742

https://www.cve.org/CVERecord?id=CVE-2022-41742

- CVE-2023-0567

https://www.cve.org/CVERecord?id=CVE-2023-0567

- CVE-2023-0568

https://www.cve.org/CVERecord?id=CVE-2023-0568

- CVE-2023-0662

https://www.cve.org/CVERecord?id=CVE-2023-0662

- CVE-2023-31124

https://www.cve.org/CVERecord?id=CVE-2023-31124

- CVE-2023-31130

https://www.cve.org/CVERecord?id=CVE-2023-31130

- CVE-2023-31147

https://www.cve.org/CVERecord?id=CVE-2023-31147

- CVE-2023-32067

https://www.cve.org/CVERecord?id=CVE-2023-32067

- CVE-2023-3823

https://www.cve.org/CVERecord?id=CVE-2023-3823

- CVE-2023-3824

https://www.cve.org/CVERecord?id=CVE-2023-3824

- CVE-2023-44487

https://www.cve.org/CVERecord?id=CVE-2023-44487

- CVE-2023-51385

https://www.cve.org/CVERecord?id=CVE-2023-51385

- CVE-2024-2511

https://www.cve.org/CVERecord?id=CVE-2024-2511

- CVE-2024-39515

https://www.cve.org/CVERecord?id=CVE-2024-39515

- CVE-2024-39516

https://www.cve.org/CVERecord?id=CVE-2024-39516

- CVE-2024-39525

https://www.cve.org/CVERecord?id=CVE-2024-39525

- CVE-2024-39526

https://www.cve.org/CVERecord?id=CVE-2024-39525

- CVE-2024-39527

https://www.cve.org/CVERecord?id=CVE-2024-39527

- CVE-2024-39534

https://www.cve.org/CVERecord?id=CVE-2024-39534

- CVE-2024-39544

https://www.cve.org/CVERecord?id=CVE-2024-39544

- CVE-2024-39547

https://www.cve.org/CVERecord?id=CVE-2024-39547

- CVE-2024-39563

https://www.cve.org/CVERecord?id=CVE-2024-39563

- CVE-2024-4741

https://www.cve.org/CVERecord?id=CVE-2024-4741

- CVE-2024-47489

https://www.cve.org/CVERecord?id=CVE-2024-47489

- CVE-2024-47490

https://www.cve.org/CVERecord?id=CVE-2024-47490

- CVE-2024-47491

https://www.cve.org/CVERecord?id=CVE-2024-47491

- CVE-2024-47493

https://www.cve.org/CVERecord?id=CVE-2024-47493

- CVE-2024-47494

https://www.cve.org/CVERecord?id=CVE-2024-47494

- CVE-2024-47495

https://www.cve.org/CVERecord?id=CVE-2024-47495

- CVE-2024-47496

https://www.cve.org/CVERecord?id=CVE-2024-47496

- CVE-2024-47497

https://www.cve.org/CVERecord?id=CVE-2024-47497

- CVE-2024-47498

https://www.cve.org/CVERecord?id=CVE-2024-47498

- CVE-2024-47499

https://www.cve.org/CVERecord?id=CVE-2024-47499

- CVE-2024-47501

https://www.cve.org/CVERecord?id=CVE-2024-47501

- CVE-2024-47502

https://www.cve.org/CVERecord?id=CVE-2024-47502

- CVE-2024-47503

https://www.cve.org/CVERecord?id=CVE-2024-47503

- CVE-2024-47504

https://www.cve.org/CVERecord?id=CVE-2024-47504

- CVE-2024-47506

https://www.cve.org/CVERecord?id=CVE-2024-47506

- CVE-2024-47507

https://www.cve.org/CVERecord?id=CVE-2024-47507