Severity

High

Analysis Summary

CVE-2022-22188 CVSS:7.5

Juniper Networks Junos OS is vulnerable to a denial of service, caused by a heap-based buffer overflow in the PFE. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to cause a device to hang.

CVE-2022-22186 CVSS:7.2

Juniper Networks Junos OS could allow a remote attacker to bypass security restrictions, caused by an improper initialization vulnerability. By sending a specially-crafted request, an attacker could exploit this vulnerability to forward packets to egress interfaces instead of discarded.

CVE-2022-22189 CVSS:7.8

Juniper Networks Contrail Service Orchestration could allow a local authenticated attacker to gain elevated privileges on the system, caused by an incorrect ownership assignment vulnerability. By sending a specially-crafted request, an attacker could exploit this vulnerability to escalate privileges.

CVE-2022-22194 CVSS:7.5

Juniper Networks Junos OS Evolved is vulnerable to a denial of service, caused by an improper check for unusual or exceptional conditions vulnerability in the packeIO daemon. By sending a specially-crafted GRE packet, a remote attacker could exploit this vulnerability to cause the PFE to restart.

CVE-2022-22187 CVSS:7.8

Juniper Networks Juniper Identity Management Service could allow a local authenticated attacker to gain elevated privileges on the system, caused by an improper privilege management vulnerability in the Windows Installer framework. By using specially-crafted binaries, an authenticated attacker could exploit this vulnerability to escalate privileges.

CVE-2022-22185 CVSS:7.5

Juniper Networks Junos OS is vulnerable to a denial of service. By sending a specific fragmented packet to the device, a remote attacker could exploit this vulnerability to cause a flowd process crash.

CVE-2022-22198 CVSS:7.5

Juniper Networks Junos OS is vulnerable to a denial of service, caused by an access of uninitialized pointer vulnerability in the SIP ALG. By sending a specially-crafted request, an attacker could exploit this vulnerability to cause a denial of service.

CVE-2022-22191 CVSS:6.5

Juniper Junos OS is vulnerable to a denial of service, caused by a flaw in the processing of a flood of specific ARP traffic. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to cause a denial of service.

Impact

- Denial of Service
- Privilege Escalation
- Security Bypass

Indicator Of Compromise

CVE

- CVE-2022-22188
- CVE-2022-22186
- CVE-2022-22189
- CVE-2022-22194
- CVE-2022-22187
- CVE-2022-22185
- CVE-2022-22198
- CVE-2022-22191

Affected Vendors

Juniper

Affected Products

- Juniper Networks Junos OS
- Juniper Networks EX4600 Series
- Juniper Networks EX4650 Series
- Juniper Networks QFX 5100 Series
- Juniper Networks Contrail Service Orchestration 6.0.0
- Juniper Networks Junos OS Evolved
- Juniper Networks PTX10003
- Juniper Networks PTX10008
- Juniper Networks PTX10004
- Juniper Networks Identity Management Service 1.1.3
- Juniper Networks Junos OS 17.3
- Juniper Networks SRX Series
- Juniper Networks MX Series
- Juniper Networks Junos OS 20.4
- Juniper Networks Junos OS 21.1
- Juniper Networks EX4300

Remediation

Refer to Juniper Networks Security Bulletin for patch, upgrade or suggested workaround information.

CVE-2022-22188

CVE-2022-22186

CVE-2022-22189

CVE-2022-22194

CVE-2022-22187

CVE-2022-22185

CVE-2022-22198

CVE-2022-22191