FEYE-2020-0020

Description

Digi International's ConnectPort X2e is susceptible to a local privilege escalation vulnerable to the privileged user `root`.

Impact

High - An attacker with remote network access to a X2e could remotely compromise the device. This could be used to install malware, modify system behavior, or stage a more serious attack.

Exploitability

Medium - An attacker would need to read and write files as the system user python. On production devices, this can be accomplished remotely by establishing an SSH connection or access via a TTY.

CVE Reference

CVE-2020-12878

Technical Details

The ConnectPort X2e performed filesystem actions as the privileged system user root on files controllable by the less-privileged user python. A malicious attacker could use this to escalate privileges from the local user `python` user to `root`.

Mandiant determined that the user `root` executed the file `/etc/init.d/S50dropbear.sh` during normal system boot. The shell script performed a `chown` on the directory `/WEB/python/.ssh/`, which was writable as the user `python`.

To exploit this, Mandiant used Linux symbolic links to force the system to set the ownership of the directory `/etc/init.d/` to `python:python`. Mandiant could then create a malicious `init` script in the `/etc/init.d/` directory that would be executed by `root` on future system boots.

Resolution

Digi International has fixed the reported vulnerability in version 3.2.30.6 (May 2020) of the ConnectPort X2e software.

Discovery Credits

- Jake Valletta, FireEye Mandiant
- Sam Sabetan, FireEye Mandiant

Disclosure Timeline

- 13 February 2020 - Issue reported to vendor
- 11 March 2020 - Issue confirmed by Digi International
- 14 May 2020 - CVE reserved with MITRE
- May 2020 - Digi Releases Patch
- 17 February 2021 - FireEye Mandiant advisory published

References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12878
- https://www.fireeye.com/blog/threat-research/2021/02/solarcity-exploitation-of-x2e-iot-device-part-one.html
- https://www.fireeye.com/blog/threat-research/2021/02/solarcity-exploitation-of-x2e-iot-device-part-two.html