NEC Security Advisory:

Vulnerabilities of UNIVERGE Communication Products

Publish Date: October 21, 2020
Revision: 1.0

Vulnerability Overview

A series of zero-day vulnerabilities have been discovered in the popular low-level TCP / IP software library developed by Treck, Inc. This vulnerabilities, given the name Ripple20.

Impact on NEC Communication Products

Most of NEC Communication Products are not impacted by these vulnerabilities at this time. The following products are currently known to be affected by the reported vulnerabilities.

- SV9300
- SV8300
- NEAX2000 IPS

Mitigation / Recommended Action

To minimize the vulnerabilities, this notice re-confirms to carry out the following recommended actions. On top of these, application of security patches will be required to remove the affected vulnerabilities.

Products;	Resolution	Affected CVE
SV9300	Apply patch software	CVE-2020-11901, CVE-2020-11912
SV8300	None Recommend to upgrade SV9300 from SV8300	CVE-2020-11901, CVE-2020-11912
NEAX2000 IPS	None	CVE-2020-11912

[Mitigation]

For UNIVERGE SV9300, please upgrade the main software to V8.2.0/V7.5.0/V6.4.0.

[Recommended Action]

- ✓ Minimize network exposure for embedded and critical devices, keeping exposure to the minimum necessary, and ensure that devices are not accessible from the Internet unless essential.
- ✓ Enable only secure remote access methods.
- ✓ Block network attacks via deep packet inspection, similar to how modern DNS server, switches, routers and firewalls drop malformed packets with no additional configuration.
- ✓ In the firewall of the customer's network environment, block communication with IP addresses other than the devices connected to the above communication servers and TCP.

These recommended actions should be carried out immediately. Please be aware that because this is an ongoing and continuous investigation, there may be additional vulnerabilities that are discovered during ongoing testing and investigation and NEC will provide updates as information becomes available. Additionally, other products that are not currently considered within this bulletin may be discovered to be affected.