NEC Security Advisory:

Vulnerabilities of UNIVERGE Communication Products

Publish Date: January 27, 2021
Revision: 2.0

Vulnerability Overview

This notice relates to security vulnerability (designated CVE-2020-5685/CVE-2020-5686) which have been found in the UNIVERGE SV9500 series and SV8500 series communication Products.
This vulnerability is the risk level of "Critical" if the products are exposed to the network without stringent security controls.

Impact on NEC Communication Products

The Telephony Server Maintenance Menu (Web based remote maintenance console, TSMM) of following products are affected by this vulnerability.

- SV9500 Appliance Model using SCF-CP02 CPU V1-V8
- SV9500 Software Model V1-V6
- SV8500 S6-S8

To successfully exploit these vulnerabilities, the attacker requires to access the products to enter certain commands.

Mitigation / Recommended Action

To minimize the vulnerabilities, this notice re-confirms to carry out four basic-practices. On the top of these, application of security patches will be required to remove the remaining vulnerabilities. The following products are the subject of this notice.

Products;	Resolution	Affected CVE
SV9500 series	Apply patch software	CVE-2020-5685, CVE-2020-5686
SV8500 series	Apply patch software	CVE-2020-5685, CVE-2020-5686

[Basic Practices]

- ✓ 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 the TSMM.

[Security patches]

UNIVERGE SV9500 V8 4.0/V7 8.0/V6 6.0	available now
UNIVERGE SV8500 S8 6.0	available now

These basic practices should be carried out immediately. The security patch should be applied as soon as the patch software becomes available.

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.

[Credit]
These vulnerabilities are found and reported by Mr. Naphon Jaipaeng of Netassess Consulting Co., Ltd. in Thailand. We appreciate his excellent knowledge and professional approach that led us to solve the problems.