## NEC Security Advisory:

Vulnerabilities of **UNIVERGE® Communication Products for SMB**

Publish Date: Aug 31, 2020
Revision: 2.0

## Vulnerability Overview

This notice relates to 9 security vulnerabilities (designated CVE-2019-20025 to CVE-2019-20033) which have been found in the UNIVERGE communication Products for SMB platform. These vulnerabilities are the risk level of "Critical" if the products are exposed to the outside network without stringent security controls, for example, using D-NAT (destination network address translation) setting to the Internet router. Even though the products are separated from the outside network, the vulnerabilities still remain at a risk level of "High".

## Mitigation / Recommended Action

To successfully exploit these vulnerabilities, the attacker requires to access the products to enter certain commands and/or certain dialing patterns.

To minimize the vulnerabilities, this notice re-confirms to carry out three 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.

- UNIVERGE SV9100
- UNIVERGE SV8100
- SL2100
- SL1100/SL1000
- UNIVERGE UM8000
- UNIVERGE UM4730

The following basic practice no.1 is the security measure to be applied at the router, the others are the security measures to be applied to the products listed above.

[Basic Practices]

1. Do not set a static port forwarding to the router which allows access to the product from the outside network.
2. Change the passwords and security related dial-access-codes from the defaults to ones that are hard to guess.
3. Disable all unused features.

[Security patches]

1. Apply the security patch software provided by NEC platforms.
   The schedule of the patch software for each product is as follows

| | | | |
|---|---|---|---|
| • UNIVERGE SV9100(CP10/CP20) | Ver.10.60.53 | available now | |
| • UNIVERGE SV8100 | Ver.10.32 | available now | (Asia, Australia, LASC) |
| | Ver.9.71 | available now | (EMEA) |
| | Ver.11.12 | available now | (US) |
| • SL2100 | Ver.2.30.02 | available now | |
| • SL1100/SL1000 | Ver.7.21 | available now | |
| • UNIVERGE UM8000 | Ver.11.10.1.17 | available now | |
| • UNIVERGE UM4730 | Ver.11.10.1.17 | 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.