Vulnerability Report on Improper Restriction of XML External Entity Reference in NB-Designer

Release date: January 14, 2025
OMRON Corporation

■Overview

We found a vulnerability Improper Restriction of XML External Entity Reference (CWE-611) in NB-series NX-Designer. Attackers may be able to abuse this vulnerability to disclose confidential data on a computer.

The products and versions affected by these vulnerabilities, mitigation and protection measures are shown below. Make sure to implement these recommended mitigations and protections to minimize the risk of exploitation of these vulnerabilities. Moreover, to ensure that customers use our products with confidence, the security enhanced countermeasure version of each product has been prepared. Please check countermeasures shown below in this document and implement appropriate countermeasures.

■Affected products

Affected products and versions are below.

Programable Terminals NB-Designer

Model	Version
NB-Designer	Ver.1.63 or lower

Refer to the appendix for how to check the target product version.

- Programmable Terminals NB-Designer Operation Manual (V106)

■Description

Due to the vulnerability known as Improper Restriction of XML External Entity Reference (CWE-611) which exist in NX-Designer, attackers may be able to disclose confidential data on a computer.

■CVSS Scores

Improper Restriction of XML External Entity Reference (CWE-611)

CVE-2024-12298

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N Base Score 5.5

■Countermeasure

The countermeasure against the vulnerabilities can be implemented by updating each product to the countermeasure version. The countermeasure version and respective release date for each product is shown in the table below.

Programable Terminals NB-Designer

Model	Version	Release date
NB-Designer	Ver.1.64 or higher	December 16, 2024

For information on how to obtain and update the countermeasure version of the product, please contact our sales office or distributors.

■Mitigations and Protections

OMRON recommends that customers take the following mitigation measures to minimize the risk of exploitation of these vulnerabilities.

1. Anti-virus protection
   Protect any PC with access to the control system against malware and ensure installation and maintenance of up-to-date commercial grade anti-virus software protection.

2. Security measures to prevent unauthorized access
   - Minimize connection of control systems and equipment to open networks, so that untrusted devices will be unable to access them.
   - Implement firewalls (by shutting down unused communications ports, limiting communications hosts) and isolate them from the IT network.
   - Use a virtual private network (VPN) for remote access to control systems and equipment.
   - Use strong passwords and change them frequently.
   - Install physical controls so that only authorized personnel can access control systems and equipment.
   - Scan virus to ensure safety of any USB drives or similar devices before connecting them to systems and devices.
   - Enforce multifactor authentication to all devices with remote access to control systems and equipment whenever possible.

3. Data input and output protection
   Validation processing such as backup and range check to cope with unintentional modification of input/output data to control systems and devices.

4. Data recovery

   Periodical data backup and maintenance to prepare for data loss.

■Contact information

Please contact our sales office or distributors.

https://www.ia.omron.com/global_network/index.html

■Acknowledgments

We are grateful for the commitment of Mr. Michael Heinzl to finding and reporting this vulnerability through JPCERT/CC.

■Update history

- January 14, 2025: New Release