An official website of the United States government Here's how you know

TLP:WHITE

ICS Advisory (ICSA-21-257-09)

More ICS-CERT Advisories

Siemens NX

Original release date: September 14, 2021

Legal Notice

All information products included in https://us-cert.cisa.gov/ics are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see https://us-cert.cisa.gov/tlp/.

1. EXECUTIVE SUMMARY

- **CVSS v3 7.8**
- **ATTENTION:** Low attack complexity
- **Vendor:** Siemens
- **Equipment:** NX
- **Vulnerabilities:** Use After Free, Out-of-bounds Read

2. RISK EVALUATION

Successful exploitation of these vulnerabilities could lead to an access violation and to arbitrary code execution on the target host system.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of NX are affected:

- NX 1980 Series: All versions prior to v1984

3.2 VULNERABILITY OVERVIEW

3.2.1 USE AFTER FREE CWE-416

The IFC adapter in the affected application contains a use-after-free vulnerability, which could be triggered while parsing user-supplied IFC files. An attacker could leverage this vulnerability to execute code in the context of the current process.

CVE-2021-37202 has been assigned to this vulnerability. A CVSS v3 base score of 7.8 has been calculated; the CVSS vector string is (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H).

3.2.2 OUT-OF-BOUNDS READ CWE-125

The plmxmlAdapterIFC.dll contains an out-of-bounds read while parsing user supplied IFC files, which could result in a read past the end of an allocated buffer. This could allow an attacker to cause a denial-of-service condition or read sensitive information from memory locations.

CVE-2021-37203 has been assigned to this vulnerability. A CVSS v3 base score of 7.1 has been calculated; the CVSS vector string is (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H).

3.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Critical Manufacturing
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** Germany

3.4 RESEARCHER

Siemens reported these vulnerabilities to CISA.

4. MITIGATIONS

Siemens has identified the following specific workarounds and mitigations users can apply to reduce the risk:

- Avoid opening files from unknown sources in NX
- Update to v1984 or later version (login required)

As a general security measure, Siemens strongly recommends users protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends users configure the environment according to Siemens operational guidelines for industrial security and follow the recommendations in the product manuals.

Additional information on industrial security by Siemens can be found at: https://www.siemens.com/industrialsecurity

For more information about this issue, please see Siemens Security Advisory SSA-208530

CISA recommends users take the following measures to protect themselves from social engineering attacks:

- Do not click web links or open unsolicited attachments in email messages.
- Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.

- Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on us-cert.cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on us-cert.cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to CISA for tracking and correlation against other incidents.

No known public exploits specifically target these vulnerabilities. These vulnerabilities are not exploitable remotely.

Contact Information

For any questions related to this report, please contact the CISA at:

Email: CISAservicedesk@cisa.dhs.gov
Toll Free: 1-888-282-0870

For industrial control systems cybersecurity information: https://us-cert.cisa.gov/ics
or incident reporting: https://us-cert.cisa.gov/report

CISA continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.

This product is provided subject to this Notification and this Privacy & Use policy.