# SSA-328042: File Parsing Vulnerabilities in OBJ Translator in NX

Publication Date: 2021-11-09
Last Update: 2021-11-09
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

## SUMMARY

Siemens NX is affected by two vulnerabilities that could be triggered when the application reads OBJ files. If a user is tricked to open a malicious file with the affected application, this could lead to an access violation, and potentially also to arbitrary code execution on the target host system.

Siemens has released updates for the NX and recommends to update to the latest version. Siemens recommends to avoid opening of untrusted files from unknown sources.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| NX 1953 Series:<br>All versions < V1973.3700 | Update to V1973.3700 or later version<br>https://support.sw.siemens.com/<br>See further recommendations from section Workarounds and Mitigations |
| NX 1980 Series:<br>All versions < V1988 | Update to V1988 or later version<br>https://support.sw.siemens.com/<br>See further recommendations from section Workarounds and Mitigations |

## WORKAROUNDS AND MITIGATIONS

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

- Avoid opening files from unknown sources in NX

## GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

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

## PRODUCT DESCRIPTION

NX software is an integrated toolset that helps to develop design, simulation, and manufacturing solutions by supporting various aspects of product development allowing the designer to optimize shape to achieve a multidisciplinary design.

  

## VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

### Vulnerability CVE-2021-41535

The affected application contains a use-after-free vulnerability while parsing OBJ files.

An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13771).

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2021-41538

The affected application is vulnerable to information disclosure by unexpected access to an uninitialized pointer while parsing user-supplied OBJ files.

An attacker could leverage this vulnerability to leak information from unexpected memory locations (ZDI-CAN-13770).

| | |
|---|---|
| CVSS v3.1 Base Score | 3.3 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:T/RC:C |
| CWE | CWE-824: Access of Uninitialized Pointer |

## ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

## HISTORY DATA

V1.0 (2021-11-09): Publication Date

## TERMS OF USE