SSA-088132: Denial of Service Vulnerability in the OPC UA Server Implementations of Several Industrial Products

Publication Date: 2024-07-09
Last Update: 2024-07-09
Current Version: V1.0
CVSS v3.1 Base Score: 5.3

SUMMARY

Unified Automation .NET based OPC UA Server SDK before 3.2.2 used in several industrial products are affected by a similar vulnerability as documented in CVE-2023-27321 for the OPC Foundation UA .NET Standard implementation. A successful attack may lead to high load situation and memory exhaustion, and may block the OPC UA server.

Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC Energy Manager Basic: All versions < V7.5 affected by CVE-2023-52891	Update to V7.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109827289/ See further recommendations from section Workarounds and Mitigations
SIMATIC Energy Manager PRO: All versions < V7.5 affected by CVE-2023-52891	Update to V7.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109827289/ See further recommendations from section Workarounds and Mitigations
SIMATIC IPC DiagBase: All versions affected by CVE-2023-52891	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC DiagMonitor: All versions affected by CVE-2023-52891	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMIT V10: All versions affected by CVE-2023-52891	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMIT V11: All versions < V11.1 affected by CVE-2023-52891	Update to V11.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109820441/ 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:

- CVE-2023-52891:
  - Disable the OPC UA server in the affected product, if possible and OPC UA is not used
  - Restrict access to the OPC UA interface to trusted clients

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

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

SIMATIC Energy Manager provides users with a scalable, non-sector-specific energy data management system.

SIMATIC IPC DiagBase diagnostics software allows to recognize early on any potential faults on SIMATIC IPCs and helps to avoid or reduce system downtimes.

SIMATIC IPC DiagMonitor monitors, reports, visualizes and logs the system states of the SIMATIC IPCs. It communicates with other systems and reacts when events occur.

SIMIT Simluation Platform allows the simulation of plant setups in order to anticipate faults in the early planning phase.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2023-52891

Unified Automation .NET based OPC UA Server SDK before 3.2.2 used in Siemens products are affected by a similar vulnerability as documented in CVE-2023-27321 for the OPC Foundation UA .NET Standard implementation. A successful attack may lead to high load situation and memory exhaustion, and may block the server.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
CWE	CWE-1325: Improperly Controlled Sequential Memory Allocation

ADDITIONAL INFORMATION

For more information regarding the impact of this issue to the Unified Automation .NET based OPC UA Server SDK, refer to entry #25 in https://www.unified-automation.com/support/security-process.html.

For more information regarding the related CVE-2023-27321 refer to https://files.opcfoundation.org/SecurityBulletins/OPC%20Foundation%20Security%20Bulletin%20CVE-2023-27321.pdf.

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 (2024-07-09): Publication Date

TERMS OF USE