

## SSA-481506: Information Disclosure Vulnerability in SIMATIC S7-200 SMART Devices

Publication Date: 2024-06-11  
Last Update: 2024-06-11  
Current Version: V1.0  
CVSS v3.1 Base Score: 8.2  
CVSS v4.0 Base Score: 8.8

### SUMMARY

SIMATIC S7-200 SMART devices contain an information disclosure vulnerability which leaves the system susceptible to a family of attacks which rely on the use of predictable IP ID sequence numbers as their base method of attack and eventually could allow an attacker to create a denial of service condition.

Siemens recommends specific countermeasures for products where fixes are not, or not yet available.

### AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-200 SMART CPU CR40 (6ES7288-1CR40-0AA0): All versions affected by <a href="#">CVE-2024-35292</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-200 SMART CPU CR60 (6ES7288-1CR60-0AA0): All versions affected by <a href="#">CVE-2024-35292</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-200 SMART CPU SR20 (6ES7288-1SR20-0AA0): All versions affected by <a href="#">CVE-2024-35292</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-200 SMART CPU SR20 (6ES7288-1SR20-0AA1): All versions affected by <a href="#">CVE-2024-35292</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-200 SMART CPU SR30 (6ES7288-1SR30-0AA0): All versions affected by <a href="#">CVE-2024-35292</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-200 SMART CPU SR30 (6ES7288-1SR30-0AA1): All versions affected by <a href="#">CVE-2024-35292</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-200 SMART CPU SR40 (6ES7288-1SR40-0AA0): All versions affected by <a href="#">CVE-2024-35292</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>

SIMATIC S7-200 SMART CPU SR40 (6ES7288-1SR40-0AA1): All versions affected by <a href="#">CVE-2024-35292</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-200 SMART CPU SR60 (6ES7288-1SR60-0AA0): All versions affected by <a href="#">CVE-2024-35292</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-200 SMART CPU SR60 (6ES7288-1SR60-0AA1): All versions affected by <a href="#">CVE-2024-35292</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-200 SMART CPU ST20 (6ES7288-1ST20-0AA0): All versions affected by <a href="#">CVE-2024-35292</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-200 SMART CPU ST20 (6ES7288-1ST20-0AA1): All versions affected by <a href="#">CVE-2024-35292</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-200 SMART CPU ST30 (6ES7288-1ST30-0AA0): All versions affected by <a href="#">CVE-2024-35292</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-200 SMART CPU ST30 (6ES7288-1ST30-0AA1): All versions affected by <a href="#">CVE-2024-35292</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-200 SMART CPU ST40 (6ES7288-1ST40-0AA0): All versions affected by <a href="#">CVE-2024-35292</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-200 SMART CPU ST40 (6ES7288-1ST40-0AA1): All versions affected by <a href="#">CVE-2024-35292</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-200 SMART CPU ST60 (6ES7288-1ST60-0AA0): All versions affected by <a href="#">CVE-2024-35292</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-200 SMART CPU ST60 (6ES7288-1ST60-0AA1): All versions affected by <a href="#">CVE-2024-35292</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>

## **WORKAROUNDS AND MITIGATIONS**

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

- Restrict access to the network where the affected products are located by introducing strict access control mechanisms

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**

The S7-200 SMART series is a line of micro-programmable logic controllers that can control a variety of small automation applications.

## **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-2024-35292**

Affected devices are using a predictable IP ID sequence number. This leaves the system susceptible to a family of attacks which rely on the use of predictable IP ID sequence numbers as their base method of attack and eventually could allow an attacker to create a denial of service condition.

CVSS v3.1 Base Score	8.2
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:T/RC:C</a>
CVSS v4.0 Base Score	8.8
CVSS Vector	<a href="#">CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:H/SC:N/SI:N/SA:N</a>
CWE	CWE-330: Use of Insufficiently Random Values

## **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 (2024-06-11): Publication Date

## **TERMS OF USE**

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website ([https://www.siemens.com/terms\\_of\\_use](https://www.siemens.com/terms_of_use), hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.