Siemens Security Advisory by Siemens ProductCERT

SSA-387223: Unauthenticated Control Panel Escape Vulnerability on SIMATIC HMI Unified Comfort before V21.0

Publication Date:	2026-05-12
Last Update:	2026-05-12
Current Version:	V1.0
CVSS v3.1 Base Score:	7.7
CVSS v4.0 Base Score:	7.0

▼ SUMMARY

SIMATIC HMI Unified Comfort Panels before V21.0 are affected by a vulnerability that allows an unauthenticated attacker to access the web browser via the help link. This vulnerability allows an attacker to access the web browser through the Control Panel if it is not protected by the corresponding security mechanisms. This opens the possibility for the attacker to find backdoors, which might lead to unwanted misconfigurations.

Siemens has released new versions for the affected products and recommends to update to the latest versions.

▼ KNOWN AFFECTED PRODUCTS

Un-/Collapse All

Affected Product and Versions	Remediation
SIMATIC HMI Unified Comfort Panels Hygienic family	Show more details
SIMATIC HMI Unified Comfort Panels Standard family	Show more details

▼ MITIGATIONS

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

- Disable the taskbar which can be configured in the Control Panel > System Properties > Taskbar.
- Compliance with the security guidelines is strongly recommended (specially chapter “3.2 Ending HMI runtime”, “3.4.1 Enable access protection for the Control Panel” and “3.4.2 Changing runtime autostart) https://support.industry.siemens.com/cs/ww/en/view/109481300

Product-specific remediations or mitigations can be found in the section Known Affected Products.
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

▼ VULNERABILITY DESCRIPTION

Un-/Collapse All

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-2026-27662

Affected devices do not properly restrict access to the web browser via the Control Panel when no corresponding security mechanisms are in place. This could allow an unauthenticated attacker to gain unauthorized access to the web browser, potentially enabling the discovery of backdoors, performing unauthorized actions, or exploiting misconfigurations that may lead to further system compromise.

CVSS v3.1 Base Score	7.7
CVSS v3.1 Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
CVSS v4.0 Base Score	7.0
CVSS v4.0 Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-1188: Initialization of a Resource with an Insecure Default

▼ 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	(2026-05-12):	Publication Date

▼ TERMS OF USE

The use of Siemens Security Advisories is subject to the terms and conditions listed on: https://www.siemens.com/productcert/terms-of-use.

SSA-387223 © Siemens 2026