

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- ▼ [Security Architecture](#)
  - [Cloud Security](#)
  - [Identity & Access](#)
  - [Data Protection](#)
  - [Network Security](#)
  - [Application Security](#)
- ▼ [Security Strategy](#)
  - [Risk Management](#)
  - [Security Architecture](#)
  - [Disaster Recovery](#)
  - [Training & Certification](#)
  - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [ICS/OT](#)



## ICS Patch Tuesday: Siemens, Schneider Electric Address 43 Vulnerabilities

By [Eduard Kovacs](#) on May 11, 2022

Share

Tweet

推荐 12



The 15 new advisories released by Siemens and Schneider Electric this Patch Tuesday address a total of 43 vulnerabilities, including ones that have been assigned a “critical” severity rating.

[Siemens](#) has released 12 advisories covering 35 vulnerabilities. Based on CVSS scores, the most important advisory covers 11 flaws affecting the web server of SICAM P850 and P855 devices.

One of these bugs is critical and it allows an unauthenticated attacker to execute arbitrary code or launch a denial-of-service (DoS) attack. The five high-severity vulnerabilities covered by the advisory can lead to DoS attacks, code execution, traffic capturing and interfering with device functionality, cross-site scripting (XSS) attacks, or access to a device's management interface.

Critical and high-severity vulnerabilities have also been found in Desigo PXC3, PXC4, PXC5 and DXR2 devices. These flaws can be exploited for arbitrary code execution, and password spraying or credential stuffing attacks.

High-severity code execution issues have been identified in Simcenter Femap, JT2Go and Teamcenter Visualization, and various Siemens industrial products that use the cURL library.

**Learn more about vulnerabilities in industrial systems at**

## [SecurityWeek's ICS Cyber Security Conference](#)

High-severity flaws that can be leveraged for DoS attacks have been discovered in Desigo DXR and PXC controllers, the CP 44x-1 RNA communication processor modules, Teamcenter, and various industrial products that use OPC Local Discovery Server.

A high-severity vulnerability that can be exploited by an authenticated attacker to escape the Kiosk Mode in SIMATIC WinCC has also been disclosed.

Siemens has started releasing patches for these vulnerabilities, but fixes are currently not available for all impacted products.

[Schneider Electric](#) has released three advisories to inform customers about eight vulnerabilities. Six of these flaws affect some Wiser Smart home automation products, including a critical hardcoded credentials issue, and high-severity vulnerabilities that can be exploited for brute-force attacks, admin account hijacking, cross-domain attacks, and obtaining authentication credentials.

The company has also informed customers about a medium-severity DoS vulnerability in Saitel DP remote terminal unit (RTU) products, and a high-severity remote code execution flaw in the PowerLogic ION Setup engineering tool for metering devices.

Schneider has released patches for Saitel DP RTU and PowerLogic ION products. In the case of Wiser Smart, the affected products have reached end of life and no longer receive patches, but the company has made available some mitigations.

**Related:** [ICS Patch Tuesday: Siemens, Schneider Fix Several Critical Vulnerabilities](#)

**Related:** [Siemens Addresses Over 90 Vulnerabilities Affecting Third-Party Components](#)

**Related:** [ICS Patch Tuesday: Siemens, Schneider Electric Address Nearly 50 Vulnerabilities](#)

[Share](#)[Tweet](#)[推荐 12](#)

Eduard Kovacs ([@EduardKovacs](#)) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia's security news reporter. Eduard holds a bachelor's degree in industrial informatics and a master's degree in computer techniques applied in electrical engineering.

Previous Columns by Eduard Kovacs:

[Hackers Can Make Siemens Building Automation Controllers 'Unavailable for Days'](#)

[Critical Vulnerability Allows Remote Hacking of Zyxel Firewalls](#)

[Critical Vulnerabilities Provide Root Access to InHand Industrial Routers](#)

[Size of Early Stage Cyber Deals Continues to Surge: DataTribe](#)

[Hundreds of Thousands of Konica Printers Vulnerable to Hacking via Physical Access](#)

[2022 ICS Cyber Security Conference | USA \[Hybrid: Oct. 24-27\]](#)

sponsored links

[Virtual Event Series - Security Summit Online Events by SecurityWeek](#)

[2022 CISO Forum: September 13-14 - A Virtual Event](#)

[2022 Singapore/APAC ICS Cyber Security Conference](#)

**Tags:**

[ICS/OT](#) [NEWS & INDUSTRY](#) [Vulnerabilities](#)