

ICS Patch Tuesday: Siemens, Schneider Electric Address Dozens of Vulnerabilities

Siemens and Schneider Electric's Patch Tuesday advisories for April 2023 address a total of 38 vulnerabilities found in their products.

The total number of vulnerabilities is significantly smaller than in February and March, when the industrial giants addressed roughly 100 security issues.

Siemens

Siemens has published 14 new advisories that cover a total of 26 vulnerabilities. Some issues have been patched, but for others only workarounds and mitigations are available, and the company does not plan on releasing fixes for some of the impacted products.

The most serious appears to be CVE-2023-28489, a critical vulnerability affecting Sicam A8000 series remote terminal units (RTUs), which are designed for telecontrol and automation in the energy supply sector.

The vulnerability can allow an unauthenticated attacker to execute arbitrary commands on the targeted device, but attacks are only possible if the device is configured to allow remote operation, which is disabled by default. Siemens has released patches for this security hole.

Siemens has also informed customers about three high-severity DoS vulnerabilities affecting the web server present in multiple Simatic industrial products.

Siprotec 5 devices are affected by a DoS vulnerability that can be exploited by an unauthenticated attacker by sending malicious requests to the targeted system.

Several high-severity flaws disclosed by Siemens are related to the parsing of specially crafted files, which can often lead to arbitrary code execution. An attacker can exploit these vulnerabilities by getting a user to open a malicious file.

Impacted products include JT Open Toolkit, JT Utilities, Teamcenter Visualization, JT2Go, and TIA Portal.

[Read: Counting ICS Vulnerabilities: Examining Variations in Numbers Reported by Security Firms]

Siemens has also informed customers about issues affecting third-party components, including critical and/or high-severity bugs in the Wind River VxWorks real-time operating system, the Linux kernel, OPC Foundation Local Discovery Server (LDS), Luxion's KeyShot, and various libraries.

Vulnerable versions of these third-party components are used in products such as Scalance XCM332 switches, Solid Edge, and Simatic products.

Exploitation of these flaws can lead to arbitrary code execution, DoS attacks, privilege escalation, and information disclosure.

Medium-severity vulnerabilities related to weak encryption and other information-exposure issues have been addressed by Siemens in Scalance X-200IRT, Simatic industrial PCs, Mendix, and the Polarion application lifecycle management (ALM) products.

Schneider Electric

Schneider Electric has released six new advisories covering a dozen vulnerabilities. The company has made available patches

for most of the flaws and has shared mitigations for the issues it has yet to fix with updates.

The most important advisory, based on CVSS scores, covers two critical and one-high severity vulnerabilities affecting APC and Schneider-branded Easy UPS online monitoring software. Exploitation can lead to remote code execution or a DoS condition.

Customers have also been informed about a high-severity code execution issue in InsightHome and InsightFacility smart edge devices for solar and storage systems. However, exploitation requires authentication.

Remote code execution and DoS flaws have been found in the EcoStruxure Control Expert software for Modicon PLCs and PACs. In addition, DoS bugs have been found in some of the Modicon PLCs and PACs themselves.

Schneider has also informed customers about third-party component vulnerabilities, specifically three high-severity issues affecting its controllers due to the use of Codesys components.

A medium-severity issue that can allow a local attacker to execute code during the installation process has been patched in the Easergy Builder installer for T300, Saitel DR and Saitel DP products.

Related: 2023 ICS Patch Tuesday Debuts With 12 Security Advisories From Siemens, Schneider

Related: Siemens Drives Rise in ICS Vulnerabilities Discovered in 2022: Report

ICS Patch Tuesday: Siemens, Schneider Electric Address Dozens of Vulnerabilities