ICS Patch Tuesday: Siemens, Schneider Electric Address Nearly 50 Vulnerabilities

By Eduard Kovacs on February 09, 2022

Industrial giants Siemens and Schneider Electric released a total of 15 advisories on Tuesday to address nearly 50 vulnerabilities discovered in their products.

Siemens

Siemens has released nine advisories addressing 27 vulnerabilities. Based on CVSS score, the most important, with a “critical” severity rating, is CVE-2021-45106. This flaw, related to hardcoded credentials, exposes the database associated with the SICAM TOOLBOX II engineering solution.

Another important advisory describes three high-severity denial-of-service (DoS) vulnerabilities that can be exploited without authentication to target the company’s controllers.

High-severity security holes have also been fixed in SIMATIC, SINEMA and SCALANCE products, which all use the same third-party strongSwan component. While these flaws have been confirmed to allow DoS attacks, one of them may also allow remote code execution in certain circumstances.

Vulnerabilities that can be exploited by tricking the targeted user into opening a specially crafted file have been patched or mitigated in Solid Edge, JT2Go, Teamcenter Visualization, and Simcenter Femap. An attacker could exploit these weaknesses for DoS attacks or remote code execution.

Siemens has also released an advisory to inform customers about a high-severity OpenSSL flaw affecting many of its products. While patches are available for some products, for others the vendor has only made available mitigations and it does not plan on releasing updates.

Medium-severity issues have been addressed in SINEMA Remote Connect Server, Spectrum Power 4, and SIMATIC WinCC and PCS.

Schneider Electric

Schneider Electric has published six advisories describing 20 vulnerabilities.

A total of eight issues, many rated "critical" and "high severity," have been found in the Interactive Graphical SCADA System (IGSS), which is used for monitoring and controlling industrial processes. The flaws can lead to remote code execution, data disclosure, and loss of control over the SCADA system.

The vulnerabilities were discovered by Tenable and Vyacheslav Moskvin, who reported his findings through Trend Micro's Zero Day Initiative (ZDI). While ZDI has yet to make its advisories public, Tenable has already released technical information and proof-of-concept (PoC) exploits.

Critical and high-severity issues have also been found in Schneider's spaceLYnk, Wiser For KNX, and fellerLYnk products.

Schneider has also released advisories to describe high- and medium-severity vulnerabilities in its EcoStruxure EV Charging Expert, Easergy P40, Harmony/Magelis iPC, and EcoStruxure Geo SCADA Expert products. Exploitation of these weaknesses could lead to unauthorized system access, local privilege escalation, disruptions, or loss of protection.

Related: ICS Patch Tuesday: Siemens, Schneider Electric Address 40 Vulnerabilities

Related: ICS Patch Tuesday: Siemens and Schneider Electric Address Over 50 Vulnerabilities

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:
University Project Cataloged 1,100 Ransomware Attacks on Critical Infrastructure
Hamas Cyberspies Return With New Malware After Exposure of Operations
ICS Patch Tuesday: Siemens, Schneider Electric Address Nearly 50 Vulnerabilities
Adobe Patches 13 Vulnerabilities in Illustrator
Critical Flaws Expose Mimosa Wireless Broadband Devices to Remote Attacks

Tags: