  - 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 Over 80 Vulnerabilities

By Eduard Kovacs on June 14, 2022

Share 发推 推荐 0 RSS

Siemens and Schneider Electric have released their Patch Tuesday advisories for June 2022. The industrial giants have addressed a total of more than 80 vulnerabilities affecting their products.

Siemens

Siemens has released 14 advisories covering 59 vulnerabilities. Thirty of these flaws, including many rated “critical” and “high severity,” impact SINEMA Remote Connect Server. The security holes, many of which affect third-party components, can lead to remote code execution, authentication bypass, privilege escalation, command injection and information disclosure.

Several critical vulnerabilities, some of which can be exploited without authentication, have been found and patched in the SICAM GridEdge application.

A critical issue related to hardcoded credentials has been resolved in Teamcenter, but the affected component is not installed by default.

Learn more about vulnerabilities in industrial systems at

SecurityWeek’s ICS Cyber Security Conference

Critical vulnerabilities have also been found in third-party components used by the SCALANCE LPE9000 local processing engine. In addition, some Apache HTTP server vulnerabilities, including critical bugs, have been found to impact RUGGEDCOM, SINEC and SINEMA products.

High-severity flaws have been found in Spectrum Power, Mendix, EN100, SCALANCE LPE9403, SINUMERIK Edge, and Xpedition Designer products. In addition, a high-severity DoS vulnerability in OpenSSL has been found to impact tens of Siemens products, but patches have yet to be released for most of them.

Medium-severity issues have been fixed in Teamcenter Active Workspace, SCALANCE XM-400 and XR-500 devices, and SINEMA Remote Connect Server.

For many of these vulnerabilities, Siemens has only released mitigations and is still working on patches.

Schneider Electric

Schneider Electric has released eight advisories to address 24 vulnerabilities identified in its products.

Seven critical flaws that could be exploited for remote code execution have been found in the Data Server module for the IGSS SCADA product.

Two critical authentication-related vulnerabilities have been found in C-Bus Home Automation products.

The industrial giant has also informed customers about four high-severity issues related to credentials and data deserialization in the StruxureWare Data Center Expert product.

Conext ComBox is affected by vulnerabilities that can lead to clickjacking, brute-force, and CSRF attacks. EcoStruxure Cybersecurity Admin Expert is affected by two high-severity bugs that can allow device spoofing and man-in-the-middle attacks.

Medium- and low-severity vulnerabilities have been found in the Geo SCADA Mobile, EcoStruxure Power Commission, and CanBRASS products.

Schneider has released patches for all of these vulnerabilities, except for Conext ComBox, which the company discontinued in January 2020. For this product, the company recommends mitigations that reduce the risk of exploitation.

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

Related: ICS Patch Tuesday: Siemens, Schneider Fix Several Critical Vulnerabilities

Share 发推 推荐 0 RSS

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:

Microsoft to Acquire Cyber Threat Analysis Company Miburo
Windows Updates Patch Actively Exploited 'Follina' Vulnerability
ICS Patch Tuesday: Siemens, Schneider Electric Address Over 80 Vulnerabilities