SECURITYWEEK NETWORK:

- Cybersecurity News
- Infosec Island
- Virtual Events

Security Experts:

WRITE FOR US

SECURITY WEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe
- 2021 CISO Forum
- ICS Cyber Security Conference
- Contact

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - IoT Security
  - Threat Intelligence
  - Endpoint Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance

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

By Eduard Kovacs on October 12, 2021

Industrial giants Siemens and Schneider Electric on Tuesday released nearly a dozen security advisories describing a total of more than 50 vulnerabilities affecting their products.

The companies have released patches and mitigations to address these vulnerabilities.

Siemens

Siemens has released 5 new advisories covering 33 vulnerabilities. The company informed customers that an update for its SINEC network management system patches 15 flaws, including ones that can be exploited for arbitrary code execution. While some of them have been assigned a *high severity* rating, exploitation requires authentication.

For its SCALANCE W1750D controller-based direct access points, Siemens released patches and mitigations covering 15 vulnerabilities, including critical weaknesses that can allow a remote, unauthenticated attacker to cause a DoS condition or execute arbitrary code on the underlying operating system. The W1750D is a brand-labeled device from Aruba, and a majority of the flaws exist in the ArubaOS operating system.

The company has also informed customers about a critical authentication vulnerability in the SIMATIC Process Historian. An attacker can exploit the flaw to insert, modify or delete data.

The two remaining advisories address high-severity denial of service (DoS) vulnerabilities in SINUMERIK controllers and RUGGEDCOM ROX devices. In the case of the RUGGEDCOM devices, an unauthenticated attacker could cause a permanent DoS condition in certain circumstances.

Schneider Electric

Schneider Electric has released 6 new advisories covering 20 vulnerabilities. One advisory describes the impact of 11 Windows flaws on the company's Conext solar power plant products. The security holes were patched by Microsoft in 2019 and 2020 and many of them have *critical* or *high* severity ratings.

Another advisory describes two critical, one high-severity and one medium-severity vulnerabilities affecting Schneider's IGSS SCADA system. The company says the worst case exploitation scenario "could result in an attacker gaining access to the Windows Operating System on the machine running IGSS in production."

The company also informed users about a high-severity information disclosure vulnerability affecting spaceLYnk, Wiser For KNX, and fellerLYnk products, and a high-severity command execution issue in the ConneXium network manager software.

The last advisory describes the impact of two AMNESIA:33 vulnerabilities on Modicon TM5 modules. AMNESIA:33 is the name assigned to 33 flaws identified last year across four open source TCP/IP stacks.

Related: ICS Patch Tuesday: Siemens and Schneider Electric Address 100 Vulnerabilities

Related: ICS Patch Tuesday: Siemens, Schneider Electric Address Over 40 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:
Apple Points to Android Malware Infections in Argument Against Sideloading on iOS
Adobe Patches Critical Code Execution Vulnerabilities in Several Products
ICS Patch Tuesday: Siemens and Schneider Electric Address Over 50 Vulnerabilities
Cloud Security Company Wiz Raises $250 Million at $6 Billion Valuation
Vulnerabilities Expose exacqVision Video Surveillance Systems to Remote Attacks