August 2021 ICS Patch Tuesday: Siemens, Schneider Address Over 50 Flaws

By Eduard Kovacs on August 12, 2021

Siemens and Schneider Electric on Tuesday released 18 security advisories addressing a total of more than 50 vulnerabilities affecting their products.

The vendors have provided patches, mitigations, and general security recommendations for reducing the risk of attacks.

Siemens

Siemens has released 10 new advisories for the August 2021 Patch Tuesday and they cover a total of 32 vulnerabilities.

Based on their assigned severity, the most important advisory is for the impact of the DNS-related vulnerabilities dubbed “NAME:WRECK” on the company’s SGT industrial gas turbines. This is not the first time Siemens has released an advisory for the impact of the NAME:WRECK flaws on its products.

Another advisory from Siemens describes a couple of high-severity vulnerabilities in the ProFTPD component of its SIMATIC CP 1543-1 and CP 1545-1 devices. The security holes can allow an attacker to remotely obtain sensitive information or execute arbitrary code.

A high severity rating has also been assigned to a missing authentication issue affecting the German industrial giant's SIMATIC S7-1200 PLCs. An attacker can exploit the flaw to bypass authentication and download arbitrary programs to the PLC.

An advisory describing vulnerabilities in JT2Go and Teamcenter Visualization covers seven flaws that can be exploited for DoS attacks, information disclosure or remote code execution. Their exploitation involves getting the targeted user to open a specially crafted file.

A separate advisory for JT2Go and Teamcenter Visualization describes two high-severity flaws that can lead to DoS or arbitrary code execution, and a medium-severity issue that can lead to information disclosure. Advisories for these products usually address many CVEs as the flaws are similar, but they are triggered using different file formats.

Another advisory that covers many CVEs — a dozen to be precise — describes the impact of vulnerabilities in Intel products on Siemens industrial systems. Siemens has released updates for several of the impacted products and is working on BIOS patches for the remaining products.

In its Solid Edge product, Siemens patched two high-severity code execution vulnerabilities that can be exploited by getting users to open specially crafted files.

The last high-severity bug addressed by the company is an OS command injection issue affecting the SINEC NMS (network management system). However, exploitation requires administrative privileges.

Schneider Electric

Schneider Electric published eight new advisories on Tuesday covering a total of 25 vulnerabilities.

The industrial giant has published two advisories describing the impact of Windows vulnerabilities on its NTZ Mekhanotronika Rus control panels. One advisory is for an HTTP protocol stack remote code execution vulnerability, which Microsoft patched in May, and the second advisory is for two issues related to the Windows Print Spooler service, including the notorious PrintNightmare flaw.

Another advisory describes three high-severity issues introduced by the use of CODESYS industrial automation software. The flaws impact industrial control systems (ICS) from Schneider and several other major vendors.

A high severity rating has also been assigned to a Harmony HMI vulnerability that could lead to DoS or unauthorized access, to a privilege escalation issue in the Pro-face GP-Pro EX HMI screen editor and logic programming software, and to an information disclosure vulnerability in AccuSine power stabilization products.

Schneider has also published an advisory for a dozen vulnerabilities affecting AT&T Labs' compressor (XMill) and decompressor (XDemill) utilities, which are used in some of the company's EcoStruxure and SCADAPack products. The affected software is no longer supported by AT&T Labs so no patches will be released by the vendor, but Schneider does plan on addressing the issues in its own products in the future.

Cisco Talos, whose researchers discovered the vulnerabilities, has disclosed technical details for each of the flaws.

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

Related: Siemens, Schneider Electric Inform Customers About Tens of 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:

Hackers Deploying Backdoors on Exchange Servers via ProxyShell Vulnerabilities
New 'Allstar' App Enforces Security Best Practices for GitHub Projects
August 2021 ICS Patch Tuesday: Siemens, Schneider Address Over 50 Flaws
Ransomware Gang Leaks Files Allegedly Stolen From Accenture
Decryption Key for Ransomware Delivered via Kaseya Attack Made Public

Tags:

ICS/OT NEWS & INDUSTRY Vulnerabilities

Search

Get the Daily Briefing

BRIEFING

Business Email Address Subscribe