SERGEY NIVENS - FOTOLIA

Critical infrastructure firms urged to patch Schneider Electric flaws

Critical infrastructure suppliers and manufacturing firms are being urged to ensure that their systems are patched up to date, after researchers discover Schneider Electric remote code execution vulnerability

Warwick Ashford, Senior analyst

Published: **02 May 2018 13:00**

Security researchers have discovered a vulnerability in Schneider Electric's systems that could give attackers free reign over IT and operational technology (OT) systems.

The remote code execution vulnerability affects two Schneider Electric applications heavily used in manufacturing, oil and gas, water, automation and wind and solar power facilities, according to researchers at cyber exposure firm Tenable.

If exploited, the vulnerability could give cyber criminals complete control of the underlying system, the researchers warn. Attackers would also be able to use the compromised system to move laterally through the network, exposing additional systems to attack, including human-machine interface (HMI) clients.

In a worst case scenario, attackers could use the vulnerability to disrupt or even cripple plant operations, the researchers said, urging all organisations that use Schneider Electric's InduSoft Web Studio and InTouch Machine Edition software to ensure their systems are patched up to date.

InduSoft Web Studio is an automation tool used to develop HMIs, supervisory control and data acquisition (Scada) systems and embedded instrumentation solutions that connect OT with the internet or corporate intranets.

InTouch Machine Edition is a scalable HMI client. This software is commonly deployed across several heavy industries, including manufacturing, oil and gas and automotive.

"A remote attacker without credentials can use this vulnerability to execute arbitrary code on vulnerable systems, potentially leading to full compromise of the InduSoft Web Studio or InTouch Machine Edition server machine," the researchers warned.

With the growing adoption of distributed and remote monitoring in industrial environments, OT and IT are converging, the researchers said, adding that as OT becomes increasingly connected, these safety-critical systems are increasingly vulnerable to cyber attacks.

News of this discovery comes just weeks after the UK's National Cyber Security Centre (NCSC,) the US Department of Homeland Security and the FBI issued a joint warning about Russian state-sponsored attacks against critical infrastructure.

Read more about critical infrastructure security

- 2018 could be year of critical infrastructure attacks, says report.
- US warns of cyber attacks on critical infrastructure.
- UK critical infrastructure skipping security checks.
- Airbus helps drive critical infrastructure cyber security.

As underscored by the joint warning, OT systems have become high-value targets for cyber criminals worldwide, which presents major challenges to human safety as well as ongoing productivity, uptime and efficiency.

At the same time, the researchers aid deployment of cyber security measures lag behind the digitisation of critical infrastructure, resulting in an "acute" inability to understand and represent cyber security risk accurately at any given time, creating a "massive" cyber exposure gap.

"Digital transformation has made its way to critical infrastructure, connecting once-isolated systems to the outside world," said Dave Cole, chief product officer at Tenable.

"This Schneider Electric vulnerability is particularly concerning because of the potential access it grants cyber criminals looking to do serious damage to mission-critical systems that quite literally power our communities.

"Tenable Research is focused on assessing, analysing and reducing the industry's overall cyber exposure across the modern computing environment – be it cloud, IT, IoT [internet of things] or OT. Solving this growing problem requires us to come together as an industry, and we commend Schneider Electric on the speed with which they released a patch to remediate this critical issue."

Tenable Research worked with Schneider Electric to disclose the vulnerability responsibly. Schneider Electric has released patches for both affected systems. Given the widespread prevalence and market share of the affected software in the OT space, urgent attention and response from affected users is required, the researchers said.

Read more about cyber threats

- EC to boost cyber security support and collaboration.
- UAE banks share information to combat cyber threats.
- SMEs failing to address cyber threats despite risks.
- Firms look to security analytics to keep pace with cyber threats.

Read more on Hackers and cybercrime prevention

Critical IIoT security risks cloud IoT's expansion into industry

By: **Peter Sullivan**

Schneider Electric increases rewards for edge-selling partners

By: **Simon Quicke**

As IT moves deeper into the factory the channel should follow

By: **Simon Quicke**

Schneider Electric increases support for partners selling at the Edge

By: **Simon Quicke**

Start the conversation

Share your comment

Send me notifications when other members comment.

Add My Comment

Companies need to work on ensuring their developers are satisfied with their jobs and how they're treated, otherwise it'll be ...

Link software development to measured business value creation

Companies must balance customer needs against potential risks during software development to ensure they aren't ignoring security...