- 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

GE SCADA Product Vulnerabilities Show Importance of Secure Configurations

By Eduard Kovacs on February 25, 2022

GE Digital has released patches and mitigations for two high-severity vulnerabilities affecting its Proficy CIMPLICITY HMI/SCADA software, which is used by plants around the world to monitor and control operations.

The flaws were found by industrial cybersecurity firm OTORIO, which this week published a brief blog post describing the issues. GE and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) have released separate advisories for each of the vulnerabilities.

One of the security holes, tracked as CVE-2022-23921, can be exploited for privilege escalation and remote code execution. However, successful exploitation requires access to the device running Proficy CIMPLICITY and the targeted server must not running a project and it must be licensed for projects. GE has released an update that sho this vulnerability.

“CVE-2022-23921 may allow an attacker with a limited access to the CIMPLICITY server to escalate privileges

by dropping a malicious file within the CIMPLICITY runtime project," Matan Dobrushin, VP of research at OTORIO, told *SecurityWeek*.

The second issue, identified as CVE-2022-21798, is related to the transmission of credentials in clear text. An attacker who can capture the credentials through a man-in-the-middle (MitM) attack can use them to authenticate to the HMI and obtain information about alerts and other parts of the system. GE said an attacker — in some cases — may also be able to change values in the system.

Learn More About Vulnerabilities in Industrial Products at SecurityWeek's ICS Cyber Security Conference

"Given CIMPLICITY's central role in OT environments, the two vulnerabilities introduce a huge disruptive impact potential on this operational server. We can assume that if and when attackers establish a foothold in the network, CIMPLICITY will be on top of their list," OTORIO warned in its blog post.

GE said users can prevent exploitation of CVE-2022-21798 by enabling encrypted communications. In fact, OTORIO noted that both vulnerabilities can be mitigated if the server has a secure configuration. The company noted, however, that this is often not the case.

[READ: Here's How Flaws in GE Relays Could Be Exploited in Real World Attacks]

This is not the first time OTORIO has looked into the security of GE CIMPLICITY. The company last year released an open source hardening tool designed to help organizations secure their GE CIMPLICITY systems. GE has also advised customers to use the OTORIO tool.

It's important that industrial organizations do not ignore these types of vulnerabilities. CIMPLICITY products have been targeted as part of sophisticated attacks linked to state-sponsored threat actors.

Related: InHand Router Flaws Could Expose Many Industrial Companies to Remote Attacks

Related: Over 100 GE Healthcare Devices Affected by Critical Vulnerability

Related: Profinet Vulnerability Exposes Siemens, Moxa Devices to DoS Attacks

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: