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

Critical Vulnerabilities Found in AUVESY Product Used by Major Industrial Firms

By Eduard Kovacs on October 22, 2021

A total of 17 types of vulnerabilities, including many rated *critical* and *high severity*, have been found by researchers in the Versiondog data management product made by AUVESY.

The vulnerabilities were discovered by employees of industrial cybersecurity firm Claroty and responsibly disclosed to Germany-based AUVESY, which specializes in data management for automated production. The vendor has patched all of the flaws.

The affected product, Versiondog, provides automatic backup and version control capabilities, and it can be integrated with a wide range of industrial systems. According to the vendor's website, the product has been used by major companies such as Nestle, Coca Cola, Kraft Foods, Merck, and several automotive giants.

"Versiondog runs inside some of the largest industrial enterprises in the world to automatically store software versions, document them, and securely back up data that can be compared to current error-free versions in order to ensure plants run efficiently," Claroty said in a blog post. "Any disruption or manipulation of the information handled by the product could have devastating consequences to the safety and integrity of an industrial process."

The vulnerabilities found in Versiondog include issues that can be exploited by remote attackers to bypass authentication, elevate privileges, obtain hardcoded cryptographic keys, execute arbitrary code, manipulate files and data, and cause denial of service.

The security holes have been found in the OS Server API, Scheduler, and WebInstaller components of Versiondog. Six of the vulnerabilities have been assigned a severity rating of *critical* and nine have been rated *high severity*.

According to Claroty, the vendor not only released patches for the vulnerabilities — fixes are included in version 8.1 — but also addressed the root causes of these and other security issues.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has also released an advisory to inform organizations about these vulnerabilities.

Claroty has described this as a “success story” in terms of the vulnerability disclosure process, but there have been many situations over the past years where potentially serious flaws were disclosed without patches being available, and vendors only took action after the disclosure attracted the attention of the media.

Claroty reported in August that more than 600 vulnerabilities affecting industrial control system (ICS) products were disclosed in the first half of 2021, more than 70% of which were assigned critical or high severity ratings.

Related: **Vulnerability Found in Industrial Remote Access Product From Claroty**

Related: **Vulnerability Allows Remote DoS Attacks Against Apps Using Linphone SIP Stack**

Related: **Industrial Firms Informed About Serious Vulnerabilities in Matrikon OPC Product**

Related: **Flaws in Nagios Network Management Product Can Pose Risk to Many Companies**

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:
Organizations Can Now Try Out End-to-End Encrypted Microsoft Teams Calls
Critical Vulnerabilities Found in AUVESY Product Used by Major Industrial Firms
Consumer Security Firm Aura Raises $200 Million at $2.5 Billion Valuation
Former Execs of Cybersecurity Firm GigaTrust Charged With Financial Fraud
Query.AI Raises $15 Million in Series A Funding Round

Tags:

ICS/OT NEWS & INDUSTRY Vulnerabilities

Search

Get the Daily Briefing

BRIEFING

Business Email Address Subscribe