

Organizations Notified of Remotely Exploitable Vulnerabilities in Aveva HMI, SCADA Products

Organizations that use human-machine interface (HMI) and supervisory control and data acquisition (SCADA) products from UK-based industrial software maker Aveva have been informed about the existence of several potentially serious vulnerabilities.

Security advisories published last week by Aveva and the US Cybersecurity and Infrastructure Security Agency (CISA) inform users about three vulnerabilities in the InTouch Access Anywhere HMI and Plant SCADA Access Anywhere products. Software updates that patch all vulnerabilities are available from the vendor.

CISA initially published its advisory in 2022, when it informed organizations about a single high-severity path traversal issue discovered by Jens Regel, a consultant at German cybersecurity firm Crisec. CISA has now updated its initial advisory to add information about additional flaws.

The vulnerability found by Regel, tracked as CVE-2022-23854, can allow an unauthenticated attacker with network access to the secure gateway to read files on the system outside the secure gateway web server.

The researcher told *SecurityWeek* that InTouch Access Anywhere Gateway instances are often exposed to the internet, allowing remote attackers to exploit the vulnerability directly from

the web. A Shodan search shows roughly 1,100 internet-exposed systems, but Regel believes that not all of them are affected by the flaw.

“The path traversal vulnerability makes it possible to access any files on the host system and read the content. You just have to know which path they are on,” the researcher explained. “If an attacker gains access to sensitive information, such as configuration files in which access data is stored, for example, this can become a real problem.”

He added, “No user interaction is necessary. The vulnerability can be exploited very easily using a command line tool such as curl.”

Regel actually disclosed his findings in September 2022 on the Full Disclosure mailing list, when he also released a proof-of-concept (PoC) exploit. His disclosure came after the vendor had released a hotfix for the vulnerability.

Aveva has now published an advisory describing this vulnerability, along with two other flaws affecting the InTouch Access Anywhere and Plant SCADA Access Anywhere products.

These flaws impact third-party components. One is a critical OpenSSL bug that can lead to denial-of-service (DoS) attacks or arbitrary code execution, and the other is a medium-severity issue related to the use of a vulnerable version of jQuery.

CISA has updated its 2022 advisory to add information about the OpenSSL and jQuery vulnerabilities.

[Read: Counting ICS Vulnerabilities: Examining Variations in Numbers Reported by Security Firms]

The UK’s National Cyber Security Centre (NCSC) has also been credited recently for finding a vulnerability in Aveva’s Plant

SCADA and Telemetry Server products. The government agency discovered a critical vulnerability that could allow an unauthenticated attacker to remotely read data, cause a DoS condition, and tamper with alarm states.

Advisories describing the security hole were published last week by CISA and Aveva.

The NCSC has not responded to *SecurityWeek's* questions about the Aveva vulnerabilities and its ICS vulnerability research in general. The agency was recently also credited for information exposure and command execution vulnerabilities found in Honeywell's OneWireless Wireless Device Manager product.

Related: Critical Vulnerabilities Allow Hackers to Take Full Control of Wago PLCs

Related: Critical Vulnerabilities Patched in ThingWorx, Kepware IIoT Products

<https://www.securityweek.com/organizations-notified-of-remotely-exploitable-vulnerabilities-in-aveva-hmi-scada-products/>