INTELLIGENCE UPDATE

# OT security: rising critical vulnerabilities, widespread risks


John O'Brien

25 Sep 2025

Uptime Intelligence has shown that operational technology (OT) systems are more vulnerable to cyberattacks than many data center operators realize (see *Seven fallacies of data center cybersecurity*). One-third of operators now cite phishing as the primary cause of their most impactful cyberattack, according to the Uptime Institute Data Center Security Survey 2025 (see *Cybersecurity incidents grow costlier amid persistent complexity*). This is followed by ransomware/malware (11%) and misconfigured systems (11%).

Many operators still rely on legacy OT equipment and software that may be a decade or more old — designed without modern cybersecurity protections. OT systems, such as supervisory control and data acquisition (SCADA) systems, building management systems (BMS), and programmable logic controllers (PLCs), have multiple points of vulnerability. Many rely on web consoles and internet connectivity for remote management, support, training and system updates, while analytical functions, such as predictive maintenance, often require access to cloud systems and data sharing.

Web consoles and browsers are de facto cyber targets and therefore require the highest levels of security. Despite this, many remain unencrypted and insecurely connected. Cyberattackers can exploit existing weaknesses within OT protocols to gain access to facility networks and subsequently exploit web console vulnerabilities. Once compromised, OT systems can fall victim to phishing attacks, data and code manipulations, or even system hijacks.

## OT network vulnerabilities

Air gaps that once provided security by separating IT and OT networks are no longer practical. Today, OT systems need to deliver real-time data and perform analytics across different networks, systems and platforms. They may need to integrate with IT management tools — for example, data center infrastructure management (DCIM), a configuration management database (CMDB) and IT service management (ITSM) — as well as Internet of Things (IoT) devices, such as sensors, mobile networks and IP-based cameras. This network convergence increases both complexity and risk.

Most OT systems rely on inherently insecure out-of-band messaging protocols, such as BACnet, Modbus and OPC. If these protocols are not updated or are no longer supported, existing security tools such as firewalls are unlikely to provide adequate protection. Meanwhile, the rapid expansion of OT malware and ransomware is increasing the likelihood of zero-day incidents, leading to high-risk common vulnerabilities and exposures (CVEs) that threaten facility OT and IT systems (see *Ransomware incidents on OT equipment surge*).

# OT systems hold critical data

PLCs and other industrial control systems (ICS) are typically integrated hardware and software tools. Standalone OT software products — such as SCADA and BMS — are also widely used across multi-vendor environments (see **Table 1**).

Both types of OT systems collect and store critical operational data from inside and outside the data center. SCADA, for example, may connect internal power distribution systems with external third-party energy supply systems. BMS may connect to facility cooling and security systems, as well as DCIM and ITSM tools, which often require integration into the IT network.

The data captured by an OT system likely includes:

- **Facility equipment data** used for managing cooling, power, and mechanical and electrical (M&E) systems. This includes original equipment manufacturer (OEM) device IDs, models, firmware, patches, support, warranty and maintenance information, as well as logs and configuration settings.
- **Real-time telemetry data** from sensors and IoT devices, such as air pressure and flow rates from CRAC/CRAH, water pressures from pumps, and voltages and current measurements from electrical systems.
- **Power distribution data** spanning the grid, UPS systems, generators and coolant distribution units (CDUs), which provide valuable information on capacity and availability throughout the facility.
- **Sensitive customer and operator data.**

# Rise in severity of OT vulnerabilities

For this report, Uptime Intelligence examined the CVEs attributed to four well-known data center OT product vendors: Honeywell, Johnson Controls, Schneider Electric and Siemens. These vendors proactively monitor, document and provide guidance for customers. There are dozens more OT product vendors that may be investigated in future reports.

Across these four suppliers, Uptime Intelligence discovered 88 CVEs issued between December 2024 and August 2025 — a 13% increase on the 78 identified in the previous 12 months — indicating a significant year-on-year rise (see **Table 1**).

A similar table is available in Part 1 of this series (see *DCIM vulnerabilities increase threat of cyberattacks*), which can be used for comparison purposes.

Table 1 Publicly available CVEs and average CVSS ratings (2025 vs 2024)

| Affected OT vendor | CVE advisories Dec 24 to Aug 25 | CVE advisories Jan to Dec 24 | 2025 CVSS average (1-10) CVSS v4 | 2024 CVSS average (1-10) CVSS v4 | Most commonly affected products |
|---|---|---|---|---|---|
| Honeywell | 16 | 5 | 8.0 (High) | 7.3 (High) | Niagara Framework and Niagara Enterprise Security; Experion PKS |
| Johnson Controls | 8 | 15 | 8.6 (High) | 7.7 (High) | iSTAR Ultra; exacqVision |
| Siemens | 27 | 23 | 7.2 (High) | 5.4 (Medium) | SIMATIC; SINEC |
| Schneider Electric | 37 | 35 | 7.0 (High) | 7.6 (High) | EcoStruxure PMO, EPO, PSO; Modicon |
| **Total** | **88** | **78** | **7.7** (High) | **7.0** (High) | |

*Note: This is not an exhaustive list of providers or products.*

UPTIME INSTITUTE 2025 2025 [CVE ADVISORY SOURCES: NIST NVD; CISA ICS; AND, THE FOUR VENDORS]

The average CVSS (Common Vulnerability Scoring System) rating of all identified CVEs in 2025 stands at 7.7 (High) out of 10, compared with 7.0 in 2024 — equivalent to a 10-percentage point increase in severity.

By comparison, the average CVSS score of DCIM products identified in Part 1 is 6.4 (Medium). This suggests that OT systems are significantly more vulnerable than DCIM software products.

# More OT CVEs are rated Critical

**Table 2** shows that between January and August 2025, there were seven OT CVEs rated Critical (CVSS rating of 9.0 or higher). Critical risks accounted for 8% of the total CVEs identified in 2025. By comparison, only one DCIM CVE was recognized as Critical.

Table 2 Seven OT software CVEs rated Critical, 2025

| Rank | CVSS rating | Application domain(s) | Affected OT software/ equipment | CVE and CWE references | CWE explanation (paraphrased) |
|---|---|---|---|---|---|
| 1<br>Honeywell (May 2025) | 9.9 | Industrial control, physical security | MB-Secure (before v11.04) and MB-Secure PRO (before v03.09) | CVE-2025-2605<br>CWE-78: Improper Neutralization of Special Elements used in an OS Command (OS Command Injection) | Vulnerability allows privilege abuse by an attacker, after executing malicious commands in the OT software operating system (see *Zero-trust failings put data at risk*).<br>**Risk:** increased attack exposure — lateral movement. |
| 2<br>Honeywell (Jul 2025) | 9.4 | Industrial control, IoT | Experion PKS and OneWireless WDM (multiple versions) | CVE-2025-2523;<br>CWE-191 Integer Underflow (Wrap or Wraparound) | Vulnerability allows an attacker to compromise system calculations, leading to errors, data corruption, and remote code execution.<br>**Risk:** total system compromise; denial of service. |
| 2<br>Johnson Controls (Aug 2025) | 9.4 | IT/OT/IoT, physical security | iSTAR ultra G2 SE (cyber-hardend network door controller | CVE-2025-53695<br>CWE-78: Improper Neutralization of Special Elements used in an OS Command (OS Command Injection) | Vulnerability allows an unauthenticated attacker to exploit iSTAR's web app to gain access to the operating system (OS) firmware as a root user (see *Zero-trust failings put data at risk*).<br>**Risk:** total system compromise. |
| 4<br>Johnson Controls (Aug 2025) | 9.3 | IT/OT/IoT, physical security | iSTAR ultra G2 SE | CVE-2025-53696<br>CWE-494: Download of Code Without Integrity Check | Vulnerability allows malicious downloads hidden in updates, plugins or scripts to execute on the HTTP browser, often without detection.<br>**Risk:** remote code execution. |
| 4<br>Johnson Controls (Aug 2025) | 9.3 | IT/OT/IoT, physical security | iSTAR Configuration Utility (ICU) | CVE-2025-26382<br>CWE-121: Stack-based Buffer Overflow | Vulnerability allows an attacker to flood the OT system memory with too much data, leading to memory overwrites and data loss.<br>**Risk:** system crashes; denial of service. |
| 4<br>Siemens (Sep 2025) | 9.3 | Cybersecurity, IT/OT/IoT | SIMATIC PCS neo V4.1 and v5.0 | CVE-2025-40795<br>CWE-121: Stack-based Buffer Overflow | See entry above. |
| 4<br>Siemens (Sep 2025) | 9.3 | Cybersecurity, IT/OT/IoT | SIMATIC Virtualization as a Service (SIVaaS) all versions | CVE-2025-40804<br>CWE-732: Incorrect Permission Assignment for Critical Resource | Vulnerability exposes a critical resource to the shared network, without requiring authentication. An attacker on the network could read and potentially compromise sensitive operational data, including files, directories, or configurations. |

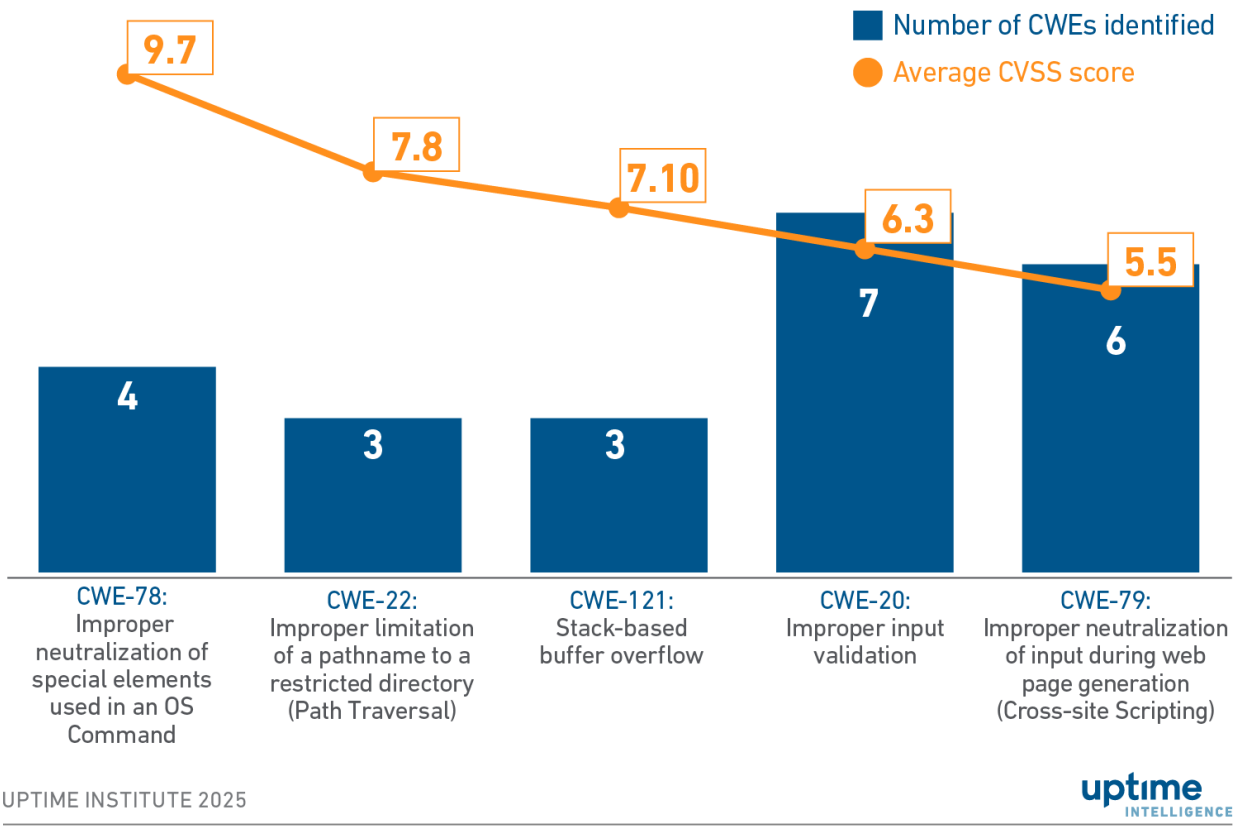
*IoT: Internet of Things*
*For all CVEs, fixes and/or mitigation advisories have been issued.*

# Zero-trust failings put data at risk

Most of the vulnerabilities identified in **Table 2** reflect common weaknesses in protecting operational and system data.

These OT systems often implicitly trust the data they receive or input by users on the network. This lack of guardrails is a zero-trust failure to verify information before it is processed. As a result, attackers may trick users into performing unsafe but "trusted" actions, which corrupt system data or — in the most serious cases — execute malicious code in the underlying OT operating system. Not only do these vulnerabilities increase the risk of malfunctions and denial-of-service (DoS) attacks, but they also significantly increase the risk of attackers pivoting to malware and ransomware exploits.

Figure 1 Most identified OT weaknesses, 2025




UPTIME INSTITUTE 2025

uptime INTELLIGENCE

**Figure 1** above highlights the five most identified OT weaknesses, all of which involve the cyberattacker(s) exploiting the OT software's implicit trust of compromised OT networks. There are two categories of exploits identified:

**Harmful data and user inputs are not recognized:**

- **CWE 20: Improper Input Validation**. The software trusts incoming data, allowing an attacker on the network to send malicious input commands without validation. This can enable changes to setpoints and thresholds, or corruption of system logic and memory.
- **CWE-22: Improper Limitation of a Pathname to a Restricted Directory (Path Traversal).** The software trusts user-supplied files or directory paths, allowing an

attacker within the system to access restricted files, such as power and cooling configurations, system logic and cryptographic keys.
- **CWE-121: Stack-based Buffer Overflow.** The software does not validate the size of data packets, such as firmware updates, enabling an attacker to overflow system memory and cause corruption, crashes, or denial-of-service (DoS) conditions.

**Harmful web inputs are not recognized:**

- **CWE-78: Improper Neutralization of Special Elements used in an OS Command (OS Command Injection).** An insecure OT web browser may allow malicious characters to be inserted into user shell command scripts. Without guardrails, attackers can perform "remote code execution" on the host operating system.
- **CWE-79: Improper Neutralization of Input During Web Page Generation (Cross-site Scripting).** The software does not prevent harmful scripts submitted through web forms and APIs (using HTML and JavaScript) from executing on a user's browser. This can allow attackers to hijack their remote web session and trick a user into clicking on a malicious link.

# Building a defense

The first line of defense should always be patching vulnerable systems to address identified vulnerabilities. However, since many OT systems may be too old to be patched, they will be at even greater risk of compromise.

Legacy systems are also unlikely to support modern cybersecurity tools, such as multi-factor authentication and single sign-on, which help prevent unauthorized access. Regardless of whether environments are new or legacy, all data center operators should ensure that fundamental security measures are in place to limit exposure:

- Eliminate the use of insecure HTTP connections to the internet.
- Enforce strict access controls. Limit access only to staff who are trusted, verified and trained on the latest vulnerabilities.
- Segregate OT networks. Route all inbound and outbound traffic so that it passes through secure gateways, where it can be sanitized or quarantined before processing.

Where possible:

- **Replace legacy OT protocols with secure versions**. These include OPC UA (for SCADA, PLC and HMI integration), Modbus/TCP Security (for SCADA and HVAC connections), BACnet/SC (for HVAC and physical security) and Secure DNP3 (for electrical and power connections).
- **Encrypt data at rest and in transit**. Use Transport Layer Security (TLS 1.3), multi-factor authentication and timely patching of all web servers.
- **Utilize real-time threat detection**. Use network and application monitoring, along with security information and event management (SIEM) tools designed specifically for OT and IoT systems.

## The Uptime Intelligence View

Uptime Intelligence's research suggests that critical OT vulnerabilities are both more common and more severe than many operators may realize. Aging legacy systems, insecure OT networks and software systems lacking protective guardrails make facility OT equipment an easy target for cybercriminals.

OT software vendors need to address these vulnerabilities by detecting, alerting and quarantining untrusted data that may contain malicious attacks.

Organizations running OT systems that are a decade or more old should consider upgrading. However, even modern OT systems are vulnerable. The growing number of CVEs demonstrate that many OT systems lack adequate cyber defenses to protect systems and data. As CVEs continue to increase in both number and severity, customers and operators will remain at high risk.

Other related reports published by Uptime Institute include:
*Cybersecurity incidents grow costlier amid persistent complexity*
*DCIM vulnerabilities increase threat of cyberattacks*
*Ransomware incidents on OT equipment surge*

## ABOUT THE AUTHOR


### John O'Brien

John is Uptime Institute’s Senior Research Analyst for Cloud and Software Automation. As a technology industry analyst for over two decades, John has been analyzing the impact of cloud migration, modernization and optimization for the past decade. John covers hybrid and multi-cloud infrastructure, sustainability, and emerging AIOps, DataOps and FinOps practices.

**jobrien@uptimeinstitute.com**

## About Uptime Institute

Uptime Institute is the Global Digital Infrastructure Authority. Its Tier Standard is the IT industry's most trusted and adopted global standard for the proper design, construction, and operation of data centers – the backbone of the digital economy. For over 25 years, the company has served as the standard for data center reliability, sustainability, and efficiency, providing customers assurance that their digital infrastructure can perform at a level that is consistent with their business needs across a wide array of operating conditions.

With its data center Tier Standard & Certifications, Management & Operations reviews, broad range of related risk and performance assessments, and accredited educational curriculum completed by over 10,000 data center professionals, Uptime Institute has helped thousands of companies, in over 100 countries to optimize critical IT assets while managing costs, resources, and efficiency.