



REPORT Q3, 2026

Catch attackers before they strike: Early warning insights for Building Automation Systems (BAS)

These insights were created by Armis Labs, a division of Armis from ServiceNow. Use of these insights is permitted provided that full attribution and linkback to the report is provided.

04

Introduction

05

From pneumatic controls to connected platforms

06

Your building is now an endpoint

06

Significant incidents

08

Top targets

09

High impact and emerging risks

10

Early warning spotlights

13

Indicators of compromise

15

Conclusion

16

About Armis Labs from ServiceNow

What makes Armis Labs different?

Armis Labs' proactive threat detection capabilities enable organizations to stay one step ahead of cyber adversaries, minimizing the risk of breaches while stopping damage before it occurs.

4200+

Armis Centrix™ for Early Warning is currently tracking over **4200 CVEs that are not published on CISA's KEV Catalog.**

Why does this matter?

28%

Once a vulnerability is published on CISA KEV, around **28% are exploited that same day.** This highlights the value of early warning insights and the need to patch quickly.

Armis Labs is now part of ServiceNow. The team behind this research keeps doing what it has always done, tracking emerging threats across connected environments worldwide, now with the reach of the ServiceNow AI platform behind it. What changes is what happens next. Findings that once ended as intelligence now become action, connecting what our researchers uncover to the workflows that prioritize it, assign it, and drive it to closure. Less distance between discovery and resolution.

[Discover ServiceNow's blueprint for Autonomous Security](#)

Introduction

On 10 August 2026, Shared Health disclosed a ransomware attack on the facility-maintenance systems at Winnipeg Health Sciences Centre, Manitoba's largest hospital. The clinical record never went down. What went down was the building: door and access control, central HVAC monitoring, badge issuance, and elevator service.

The security office closed, and the hospital posted physical guards at entrances to do the job its card readers no longer could. A week later, recovery was still in progress.

Attackers have worked out that they do not need to encrypt data, when they can seize badges, pressure the building relationships that clinical work depends on, and put operating-room climate on the table.

Building automation has become the bargaining chip, and it sits almost entirely outside the scope most healthcare security programs were built to cover. Today's BAS operate at the intersection of IT and OT worlds, creating unprecedented exposure.

As BAS converges with corporate IT networks and cloud platforms, they become both direct targets and lateral attack vectors. Organizations lack unified detection capabilities, meaning threats often go undetected until damage occurs, while simultaneously facing an accelerating vulnerability disclosure rate that outpaces remediation capacity in environments where downtime is operationally unacceptable.

BAS attacks can disable critical operational systems like HVAC, lighting, access control, fire safety, creating immediate disruption, tenant impact, and potential life-safety failures. Organizations simultaneously face tightening regulatory mandates (NIS2, NIST CSF, NERC CIP, HIPAA) that explicitly govern BAS environments, with non-compliance triggering fines and operational restrictions.

The fragmented visibility and remediation backlog create a false sense of security while real risk accumulates, forcing a choice between operational continuity and regulatory or compliance exposure.

ArmIS Labs findings:

73% Of organizations own BAS that have been used in ransomware attacks.

73% Of organizations have KEV in at least one BAS.

91% Of BAS talk over insecure protocols.

Organizations need a strategic pivot toward [autonomous security](#), including the following core principles:

- **Strive to zero exposure:** treat the exposure window itself as the metric, not ticket counts or scan coverage.
- **Shift completely left:** move remediation into design and build, not just earlier in the pipeline.
- **Secure by design:** posture is a property of how assets and workflows are created, not something bolted on afterward.
- **Continuous vulnerability detection:** replace periodic scanning with always-on detection.

The goal is not perfection; it's actively reducing the attack surface while maintaining uptime. The organizations winning this challenge are those treating BAS security as a business continuity problem first, and a technology problem second.

Research for this report was conducted in Q3, 2026 by Armis Labs security practitioners, utilizing cutting edge technology that include deception technologies, incident forensics, reverse engineering, dark web monitoring, and human intelligence to proactively identify and mitigate threats before they manifest.

From pneumatic controls to connected platforms

Building automation has roots stretching back more than a century, but the systems most facilities run today are products of a few distinct technology waves. The earliest “automation” was pneumatic compressed-air tubing driving thermostats and dampers, entirely mechanical and entirely isolated. The pivotal shift toward interoperability came with open communication standards: BACnet, first introduced in 1995 and adopted as an ISO standard in 2003, became the dominant protocol, while KNX and LonWorks emerged as widely deployed open standards, particularly across Europe.

These building automation standards and protocols were developed without security in mind, a design assumption that made sense for closed, air-gapped networks and that now defines the sector's core vulnerability.

The current generation looks nothing like its predecessors. Modern BAS are data-rich, cloud-connected platforms that fuse HVAC, lighting, access control, energy management, and fire-and-life-safety into integrated environments. Automated HVAC represents roughly 42% of deployments, followed by lighting control near 24% and security and access systems near 18%, with smart-sensor installations now exceeding a billion units worldwide.

State-of-the-art deployments increasingly run on edge controllers processing millions of data points daily, digital-twin simulation, and machine-learning diagnostics; vendors such as Honeywell, Johnson Controls, and Schneider Electric have all moved toward AI-driven, subscription-based analytics platforms over the past year.



Your building is now an endpoint

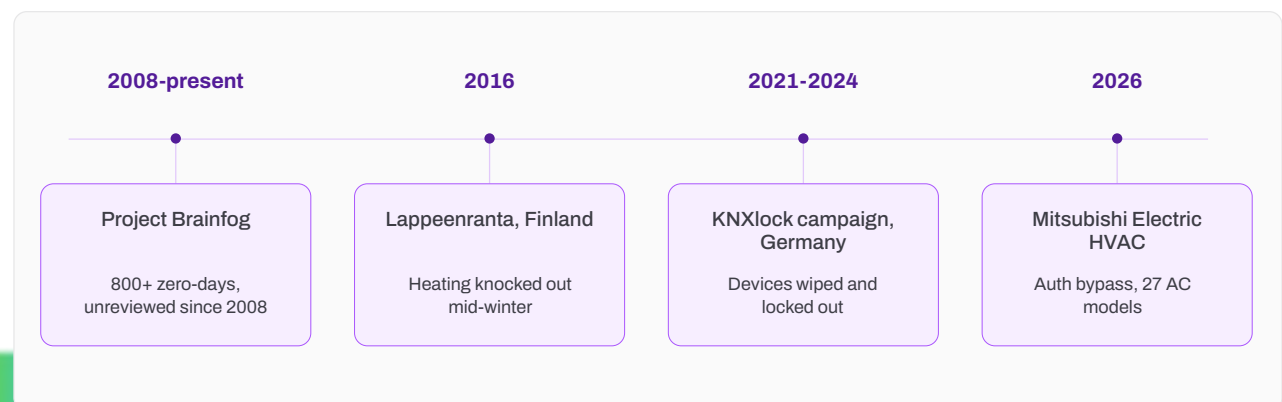
The same connectivity that makes modern BAS valuable is what makes them dangerous. Three structural problems converge:

- **Insecure-by-design protocols.** BACnet, KNX, Modbus, and similar standards were built for reliability in isolated networks, often without authentication or encryption. As these systems are exposed to the internet for remote management, decades-old protocols become attack surfaces.
- **The IT/OT convergence problem.** A BAS no longer sits in a sealed compartment. It connects to corporate IT, cloud platforms, and—in hospitals, data centers, and manufacturing, to other critical systems. That makes a compromised thermostat or HVAC controller a potential pivot point into far more sensitive networks.
- **Visibility and governance gaps.** Organizations frequently cannot inventory their own BAS devices, and ownership of BAS security is genuinely unclear—often falling between facilities management, IT, and third-party integrators. BAS incidents also tend to fly under the radar; an HVAC shutdown gets attributed to equipment failure rather than to an attacker.

In 2026 this is compounded by a collapsing discovery-to-exploitation window. AI-accelerated vulnerability research is shortening the time between a flaw being found and weaponized, while patching BAS environments remains slow because critical infrastructure cannot simply be taken offline. The remediation backlog grows faster than teams can clear it.

Significant incidents

Four well-documented incidents illustrate the range, from data theft to physical disruption:



Mitsubishi Electric HVAC flaw (2026)

A current-generation vulnerability. In February 2026, Mitsubishi Electric disclosed [CVE-2025-3699](#), a critical flaw rated CVSS 9.8 affecting 27 air-conditioning models including the AE-200 and EW-50 series; the missing-authentication issue allowed attackers to bypass authentication and gain full control over building HVAC systems.

KNXlock campaign (Germany, 2021 onward)

In October 2021, attackers reached a German office building's BAS through an unsecured UDP port exposed on the public internet, locking the operators out and rendering three-quarters of several hundred devices non-operational—affecting lighting, motion detectors, and shutter controllers. The attackers turned the system's own security feature against it, wiping devices and locking them with the KNX BCU programming key. Notably, the campaign was still ongoing into 2024, with both private and commercial building operators continuing to report compromises.

Lappeenranta, Finland (2016)

A demonstration of physical-world consequences. Between late October and November 3, 2016, the heating and hot-water systems in two buildings were knocked out by a distributed denial-of-service attack; the systems responded by repeatedly rebooting and eventually shut down, leaving residents without heat in sub-freezing conditions until controls were switched to manual.

Project Brainfog: an 18-year-old BAS codebase with 800+ zero-days still running live buildings

Gjoko Krstic of Zero Science Lab reverse-engineered ABB's Cylon Aspect and FLXeon building controllers and found American Auto-Matrix Aspect FT code from 2008 underneath. It passed to Cylon in 2013 and ABB in 2020 without meaningful security review at either handover.

He catalogued over 800 reported issues and roughly a thousand bugs: about twenty paths to root remote code execution (two unauthenticated), plus authentication bypass, SSRF, arbitrary file write, delete and traversal, undocumented backdoors, kernel buffer overflows, and default or hard-coded credentials. Firmware was downloadable from the vendor's site with no integrity controls. Scans found exposed devices in 30+ countries and 220+ cities, including airports, hospitals, government facilities, and major commercial real estate.

ABB has published CVEs for only a fraction. Its guidance says the controllers shouldn't be internet-facing, but the same stack needs connectivity for firmware updates and remote support.

The lesson: eighteen years of unreviewed security debt carried through three owners. Due diligence priced the install base and customer relationships, never the code.



Top targets

The BAS market is large, growing, and consolidates around connected, AI-enabled platforms, but its installed base carries decades of insecure-by-design technology now exposed to a faster, more automated threat landscape. The organizations managing this well are treating BAS security as a business continuity and asset visibility problem first, recognizing that the attack surface spans IT, OT, and a sprawling third-party ecosystem Here's an overview of the current top targets at risk in BAS, as identified by Armis Labs:

	HVAC systems		Chilled water plants
	Vendor remote access and integrators		Fire and life safety integrations
	Power and UPS PDU interfaces		Elevators
	Engineering workstations		BACnet systems



High impact and emerging risks

Armis Labs leverages data from over 7 billion assets through the AI-driven [Asset Intelligence Engine](#), combined with deception technology, incident forensics, reverse engineering, dark web monitoring, and human intelligence. The data we gather helps to identify exploited and emerging CVEs, as well as the dominance and impact of those attacks.

During Q3 2026 we have identified the following CVEs widely exploited in BAS:

CVE	Vendor	Criticality	First Intel Hit
CVE-2018-14916	LOYTEC	10	6/24/25
CVE-2018-14918	LOYTEC	10	8/22/24
CVE-2019-7275	Optergy	10	6/24/25
CVE-2021-31682	Automated Logic	10	6/24/25
CVE-2021-41291	ECO A	10	6/24/25
CVE-2021-41293	ECO A	10	8/22/24
CVE-2022-34753	Schneider Electric	10	1/17/24



Early warning spotlights

CVE-2018-14916

Customers using Armis Centrix™ for Early Warning were notified about this vulnerability being exploited in the wild.

At the publishing date of this report, it has not appeared in CISA's KEV Catalog, enabling them to assess their exposure and act proactively.

Armis Alert Date	CISA KEV Publish Date	Days Early
Jun 28, 2019	NA	NA

LOYTEC LGATE-902 devices with firmware 6.3.2 are vulnerable to arbitrary file deletion.

Overview

LOYTEC LGATE-902 devices running firmware 6.3.2 are affected by an arbitrary file deletion vulnerability (CVE-2018-14916). This issue is part of a cluster of vulnerabilities reported in 2019 that also included XSS and path traversal, highlighting security weaknesses in the LGATE-902 line. The vulnerability could allow deletion of arbitrary files on the device, which may affect availability and integrity.

Remediation

- **Update firmware:** Apply the latest firmware release from LOYTEC that addresses this vulnerability. Check the vendor advisories for the exact fixed version and apply to all affected LGATE-902 devices.
- **Limit exposure:** Restrict network access to LGATE-902 devices to trusted administrative networks; avoid exposing them to the internet if not required.
- **Access controls:** Ensure strong authentication and proper access controls for devices management interfaces; disable unnecessary services that may be exposed.
- **Monitor and log:** Enable and monitor file-change and deletion logs; alert on unexpected file deletions.
- **Backups and recovery:** Regularly backup configurations and important data; verify restoration procedures in case of unintended deletions.
- **Follow vendor guidance:** Review LOYTEC security advisories for additional mitigations or configuration changes specific to LGATE-902 devices.

CVE-2018-14918

Customers using Armis Centrix™ for Early Warning were notified about this vulnerability being exploited in the wild.

At the publishing date of this report, it has not appeared in CISA's KEV Catalog, enabling them to assess their exposure and act proactively.

Armis Alert Date	CISA KEV Publish Date	Days Early
Jun 28, 2019	NA	NA

Directory traversal vulnerability in LOYTEC LGATE-902 devices running firmware version 6.3.2 that could permit access to files outside the intended web root.

Overview

The CVE describes a directory traversal vulnerability affecting LOYTEC LGATE-902 devices (firmware 6.3.2), where crafting certain requests to the device's web management interface can access files outside the authorized directory. This vulnerability is part of a cluster of issues reported in 2019, including XSS and file deletion, highlighting a broader set of insecure input handling in the affected devices. The impact could include disclosure of sensitive files and potential paths for further exploitation.

Remediation

- **Action the vendor for a firmware fix:** upgrade LGATE-902 to the latest recommended firmware version that addresses directory traversal vulnerabilities.

If a patch is not yet available, implement compensating controls:

- **Restrict exposure:** block remote access to the device's management interface from untrusted networks; place the device behind a firewall or VPN; limit access to trusted admin hosts.
- **Disable or minimize exposure:** disable external management interfaces if not required; enable strict authentication controls for management access.
- **Network segmentation:** isolate the device on a dedicated management network with strict ACLs.
- **Monitoring:** enable and review logs for unusual access patterns, traversal attempts, or file access/deletion events.
- Verify configuration after upgrades and perform routine vulnerability management scans when possible.

CVE-2019-7275

Customers using Armis Centrix™ for Early Warning were notified about this vulnerability being exploited in the wild.

At the publishing date of this report, it has not appeared in CISA's KEV Catalog, enabling them to assess their exposure and act proactively.

Armis Alert Date	CISA KEV Publish Date	Days Early
July 1, 2019	NA	NA

Open Redirect vulnerability (CVE-2019-7275) in Optergy Proton/Enterprise devices allows an attacker to redirect users to arbitrary external URLs.

Overview

Optergy Proton/Enterprise devices contain an Open Redirect vulnerability identified as CVE-2019-7275. The flaw permits a redirect from the device to a user-controlled external URL without proper URL validation, which can be exploited to lure users to malicious sites or facilitate phishing attacks by masquerading as legitimate redirects within trusted workflows. The issue was disclosed in 2019 along with advisories describing open redirect risks in affected devices.

Remediation

- Apply the vendor-provided update or firmware patch addressing CVE-2019-7275. Check vendor advisories (AR-2019-008) and install the recommended security update.
- If a patch is not yet available, mitigate by disabling or restricting open redirects in the device configuration, and implement an allowlist of trusted redirect destinations to enforce strict URL validation.
- Enforce network and access controls: segment the affected devices, restrict administrative access to trusted networks, and enable comprehensive logging and monitoring for redirect attempts.
- Educate users and administrators about phishing risks associated with redirects and validate any redirects within integrated workflows.

Indicators of compromise

Below are a few concrete Indicators of Compromise (IOCs) in BAS, and their associated detection strategies. Security professionals can use these IOCs and behaviors to identify the presence of these threats in their environments.

Network / protocol

- OT ports exposed to the internet: BACnet/IP 47808, Niagara FOX/FOXS 1911/4911, KNXnet/IP 3671, Modbus/TCP 502, HTTP/S 80/443 on JACE/WebCTRL/Metasys ADS/Tracer/Niagara AX.
- BACnet Whols/I-Am bursts from a non-BMS-server, non-BBMD IP.
- WriteProperty / WritePropertyMultiple to present-value, setpoint, or out-of-service from an unexpected device ID.
- Device objects flipped out-of-service, reliability changed, or event-enable cleared (alarm suppression).
- BACnet file services (firmware/config pull) from a non-engineering station.
- New BACnet device instance numbers appearing overnight.
- New FOX sessions from non-Supervisor / non-jump-host / non-integrator IPs.
- Cleartext FOX (1911) at a claimed FOXS-only site.
- Station/Platform certificate replaced or reused across both after an unaccounted admin session.
- KNX: BCU key present where none existed; ETS download/upload blocked ("device locked"); mass unload/factory-blank across line devices; human-readable attacker-set keys (e.g. system hacked BCU key ...).

Identity / remote access

- New local users on Niagara Station, Metasys ADS/ADX, WebCTRL, or the host Windows box (admin2, reused disabled accounts, guest enabled).
- Successful auth on accounts believed disabled; disabled-account-with-blank-password access (CVE-2017-16748 family).
- Vendor VPN / TeamViewer / SimpleHelp / AnyDesk / ScreenConnect outside maintenance windows.
- Integrator account used off-hours from a new country or residential ISP.
- Password spray against /login, Niagara web login, or Metasys UI; burst of failed logins then wedged engines (CVE-2023-4486).
- API/token use on WebCTRL or Metasys not matching the operator workstation.
- Any successful head-end remote login with no work order.

Host / head-end

- New services, scheduled tasks, admin shares, or RDP on the ADS/ADX, WebCTRL server, Niagara Supervisor, or SCT/CCT box.
- SQL Express (Metasys 12–14.1) running UNION / xp_cmdshell / unexpected db_owner activity (CVE-2025-26385).
- Encryption of .bog, station backups, graphics, or historian DBs.
- Shadow copies deleted on the BMS server.
- Cobalt Strike / RMM binaries on a Niagara- or Metasys-only box.
- Unexpected outbound HTTPS/DNS from a JACE or controller.

Process / physical (pair each with: was there a change ticket?)

- Setpoint jumps (chilled water, supply air, CRAC, OR humidity) with no schedule.
- Occupancy schedules rewritten nights/weekends.
- Economizer/safeties overridden or points forced.
- Alarms disabled, or flooded then silenced.
- Doors unlock, elevator recall, or camera moves with no guard action.
- Heating/cooling loss across many zones at once.
- Manual-mode flags on a large share of equipment.
- Energy spike/crash with no weather or load change.

Platform breadcrumbs

- Niagara: download of config.bog or credential store; guest enabled or default tridium/niagara creds valid; new modules in the station; Platform connection from a non-Workbench host; syslog forwarded cleartext to a new collector.
- Metasys: new archive objects; SCT project pulled off-box; persistent XSS in UI URLs (CVE-2026-34491); SQL Express spawning new child processes.
- WebCTRL/i-Vu: file-upload writes on EOL v7.0 (CVE-2024-8525); BACnet-spoofed writes the audit log says it did not issue (CVE-2026-32666).
- Cameras/access on the facilities VLAN: Hikvision/Dahua admin adds, new users, snapshot pulls, or CVE-2021-36260 / CVE-2017-7921 traffic on the BACnet subnet.

Conclusion

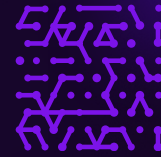
AI-assisted vulnerability research compresses the gap between discovery and weaponization, and once a flaw reaches CISA KEV, roughly 28% are exploited the same day. Armis Centrix™ for Early Warning tracks over 4,200 CVEs that never reach that catalog at all. BAS teams cannot patch at that tempo, because the equipment they protect cannot be taken offline.

More scanning will not close that gap. Move remediation into design and build. Make posture a property of how assets and workflows get created. Replace periodic scans with continuous detection. Each principle buys back time that patching alone cannot.

The organizations handling this well made one decision before they made any technology decision. They classified building automation as a business continuity system, gave it a named owner instead of leaving it between facilities, IT, and the integrator, and held it to the same standard as the clinical, trading, or production systems it quietly keeps running. The goal is not a perfect posture. It is a shrinking attack surface and uninterrupted uptime.

Key takeaways

- **Your building is an endpoint, and it is in scope.** BAS now bridges corporate IT, cloud platforms, and critical operations. A compromised HVAC controller is both a disruption tool and a pivot point into far more sensitive networks.
- **Physical consequence is the new leverage.** Ransomware that seizes badges, unlocks doors, or puts operating-room climate on the table does not need data to extract payment.
- **Insecure by design is the installed base, not the exception.** BACnet, KNX, Modbus, and LonWorks assumed an air gap that no longer exists.
- **You cannot protect what you cannot see or claim.** Most organizations cannot inventory their own BAS estate, and ownership falls into the gap between facilities, IT, and third-party integrators. Unified visibility and a named owner come first.
- **Patch cycles lost the race, so shorten the exposure window instead.** With 28% of KEV vulnerabilities exploited same-day and 4,200+ exploited CVEs never reaching KEV, early warning intelligence and continuous detection matter more than scan frequency.
- **Acquired technology carries acquired risk.** Inherited vendor stacks need a security review, not a badge change.
- **Compliance is tightening around this exact surface.** NIS2, NIST CSF, NERC CIP, and HIPAA now govern BAS environments explicitly, which turns fragmented visibility into direct regulatory exposure.



Go deep into the
platform powering
the future of security.

Explore Armis Centrix™

Armis from ServiceNow protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

+1 888 452 4011

armis.com

