Johnson Controls

Open**Blue**

Cyber Solutions

Vulnerability Management Practices

Identify, Remediate, Notify

Solution overview

Johnson Controls' Vulnerability Management Program is designed to quickly identify product vulnerabilities, address those risks with mitigations and fixes and notify our customers with timely information.

Product threat intelligence

Our Product Threat Intelligence Program actively monitors various security vulnerability feeds and submits validated issues to product teams for analysis and actions.

Industry standard CVSS 3.0 scoring

Johnson Controls uses the latest Common Vulnerability Scoring System (CVSS) and environmental scoring for all security vulnerabilities which could impact our commercially sold products.

Governed remediation

Johnson Controls has defined Service Level Agreements (SLA's) for all risk levels including critical and high vulnerabilities which are remediated before release and addressed in currently supported product versions. Our cloud-based solutions must adhere to even tighter deadlines for remediation and deployment to production.

CVE Numbering Authority

Johnson Controls practices coordinated vulnerability disclosure as a MITRE CVE® (Common Vulnerabilities and Exposures) Numbering Authority (CNA). As a CNA, Johnson Controls can self-report our product vulnerabilities to the publicly accessible National Vulnerabilities Database (https://nvd.nist.gov). This capability is incorporated into our Product Security Incident Response (PSIR) and vulnerability management processes.

CVE Numbering Authority

Product security advisories

A Product Security Advisory (PSA) communicates an issue that may impact the secure operation of a product. Instructions are provided when action is required to mitigate an identified threat. Mitigations can include configuration changes, or a software patch/update among other guidance.

ISASecure SDLA Certification

Our ISASecure SDLA Certification is a Software Development Lifecycle Assurance (SDLA) standard that is focused on the entire SDLA process in conformance with ISA/IEC 62443-4-1 ensuring that we meet the vulnerability management requirements for that standard including:

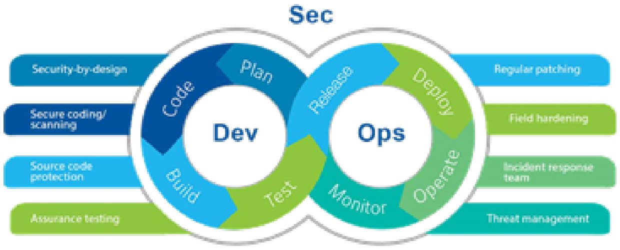
- Vulnerability testing
- Receiving security related notifications
- Assessing security related issues
- Disclosing security related issues

Zero-Trust Architecture for cloud solutions

We proactively protect our cloud solutions with a zero-trust architecture to limit the attack surface and risk that a vulnerability can be exploited. This defense-in-depth approach is an essential part of our cloud vulnerability management program.

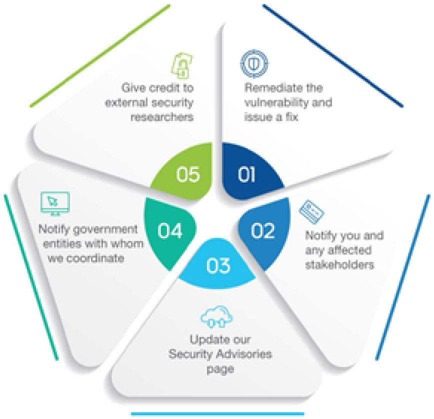
Industry best security practices for all products

Johnson Controls designs cybersecurity into all our product and solutions offerings and endeavors to protect those solutions (including software, hardware, and hosted services) and to protect your data and operations across the risk management lifecycle. Our secure product practices include the design, sourcing, development, deployment, servicing, support, and retirement of products. All new Johnson Controls commercial products are developed under governance of our cybersecurity policies, standards, and guidelines, which includes requirements for product testing and vulnerability management.



Our rapid response process

We respond to cybersecurity incidents with a disciplined process that limits your smart building's exposure by assessing impact, protecting security interests, and coordinating disclosure.


01
Remediate the vulnerability and issue a fix
02
Notify you and any affected stakeholders
03
Update our Security Advisories page
04
Notify government entities with whom we coordinate
05
Give credit to external security researchers

Outreach/memberships

Johnson Controls actively participates in cybersecurity community initiatives and is a key contributor in defining security standards and best practices for smart buildings. We maintain membership with several security organizations including, but not limited to, the following:

- International Society of Automation (ISA) Global Cybersecurity Alliance - Founding Member
- FIRST - Full member of Forum of Incident Response
- MITRE - Common Vulnerabilities and Exposure (CVE) Numbering Authority
- ISASecure Member - Strategic voting member of ISA Secure Compliance Institute

Register today to receive cybersecurity vulnerability communications:
https://www. johnsoncontrols.com/cyber-solutions/products-and-solutions/registration

Visit **https://www.** johnsoncontrols.com/cyber-solutions today to learn more about our cybersecurity approach.

Please note that this document is for customer guidance purposes only and is not legal advice. Johnson Controls is not a law firm and does not provide legal advice. While Johnson Controls products and solutions are designed for use in compliance with applicable law, implementation and deployment of Johnson Controls products and solutions should be reviewed by appropriate customer advisors and stakeholders for such compliance.

About OpenBlue

OpenBlue is a complete suite of connected solutions that serves industries from workplaces to schools, hospitals to campuses, and beyond. This platform includes tailored, AI-infused service solutions such as remote diagnostics, predictive maintenance, compliance monitoring, advanced risk assessments, and more. A dynamic new space from Johnson Controls, OpenBlue is how buildings come alive.

SS2305001