OpenBlue
Cyber Solutions

Johnson Controls

Coordinated Vulnerability Disclosure Policy

October 3, 2024

Scope – Johnson Controls provides a coordinated vulnerability disclosure service for commercially released products branded as Johnson Controls (including associated brands owned by Johnson Controls). The following solutions are not supported by the Johnson Controls' vulnerability disclosure service, even if they were purchased through Johnson Controls:

- Third-party branded products
- Pre-released products (i.e. alpha, beta versions)

Products outside of the defined support period (i.e. end-of-life/service/support) may be exempt from disclosure as they are not recommended for continued use.

Researchers welcome! – We welcome security researchers (including customers and independent organizations) to privately send reports to Johnson Controls when they believe a vulnerability is found in a Johnson Controls product. We work in partnership with responsible researchers operating in according to applicable laws, to reduce customer risk by following our coordinated vulnerability disclosure process.

Researchers will allow Johnson Controls to review their findings, develop fixes, workarounds or other corrective measures, before either party discloses any vulnerability or exploit information to the public.

Johnson Controls will communicate case status to researchers throughout the vulnerability disclosure process. If related attacks are active, Johnson Controls will work closely with the researcher to provide an early public disclosure to protect customers.

CVE ownership – Johnson Controls is a Common Vulnerability and Exposures Numbering Authority (CNA). As the CNA, Johnson Controls will own all CVE disclosures related to a Johnson Controls product. If a researcher has already engaged with CISA, they will inform CISA of our coordination and transfer the case to the one established by Johnson Controls.

Preferred Communication Language – English

Before sending report – Cybersecurity testing may be conducted on Johnson Controls solutions. We recommend that tests are conducted in a non-production test environment to protect against disruption of operations.

Product security steps outlined in the associated product Hardening Guide (Resources), must be followed before security test are executed, or they may produce field correctable findings.

The following hardening steps, if not followed, are known to result in addressable security findings:

- Update components to the most current supported release/version, and patch level that you are licensed to use, including:
  - All Johnson Controls Applications
  - All supporting software, not installed by Johnson Controls Applications, such as Windows, SQL Server, .NET and others
- Disable unused features, services, ports and software
- Install PKI certificates for applicable interfaces that are either:
  - Provided by the local IT PKI administrator
  - Acquired from a public Certificate Authority (CA)
- Before removing components not required by the Johnson Controls applications (e.g. old versions of Microsoft .NET, SQL and others):
  - Ensure the software is not needed for any other function
  - Ensure all data was properly migrated to the new Server instance

Report content – All vulnerability reports received by Johnson Controls will be treated seriously. Reports and other communications should be sent in English. The inclusion of the following elements (as currently known) will aid in the efficiency of our assessment process:

- Product name / model (or part number)*
- Product version / patch level*
- Instructions to reproduce the issue*
- Description of the findings, including deployment and configurations conditions. (Tool exports, network traces, log files and screen captures appreciated) *
- Impact of the issue, including any associated standard vulnerability descriptors:
  - Common Vulnerability and Exposures (CVEs)
  - Common Vulnerability Scoring System (CVSS) score (version 4.0 preferred)
  - Common Weakness Enumeration (CWE)
  - Common Attack Pattern Enumeration and Classification (CAPEC)
- Exploit concept and/or example code

*If these required details are not provided, we may not be able to take action.

Sending reports – If a test tool detects potential issues with a Johnson Controls component, you may share the results with Johnson Controls or report other cybersecurity concerns at this link – https://www.johnsoncontrols.com/trust-center/cybersecurity/security-advisories#ReportAVulnerability, you may also contact us at trustcenter@jci.com.

Please use our downloadable PGP key to secure communications.

Researchers grant Johnson Controls non-exclusive global, irrevocable, perpetual, sub-licensable royalty-free license to any intellectual property contained in that report or any follow-up communications to the report to analyze, commercialize, publicize, disclose, or otherwise use such intellectual property in any manner. Participating in this program does not give a Researcher any right to any intellectual property of Johnson Controls.

Reporting entities subject to this policy are required to fully cooperate with any requests by Johnson Controls for additional information and agree to coordinate vulnerability disclosures at the discretion of Johnson Controls.

Coordination timing – Johnson Controls will acknowledge receipt of reports received within 5 business days. Disclosure timeframes will be determined as part of a negotiation process to minimize customer risk. If during the process, the researcher does not respond to a request within 30 days, we may cease communications with the researcher and proceed with the process independently. Researchers must hold any reports of their findings until after Johnson Controls has published its associated Product Security Advisory and CVE.

If multiple parties are impacted, then the researcher may not share any details related to Johnson Controls' and findings related to Johnson Controls' products with the other parties without written consent.

Recognition – A Johnson Controls' public "Wall of Thanks" webpage provides optional recognition to researchers who have reported vulnerabilities which resulted in disclosure by Johnson Controls. The individual researcher names are listed by the year the associated disclosure was posted. There is no active bug bounty program.

Vulnerability Remediation – Johnson Controls aims to address each finding in a timely manner respective to the associated CVSS score. Remediation timing can be affected by dependencies, development cycles and other factors. Not all findings will result in a fix, and not all fixes may require a public disclosure.

Policy updates – Johnson Controls may update this policy without prior notice, to maintain compliance with applicable laws and regulations, industry standards, alignment with Johnson Controls policies and adherence to CNA and CISA requirements. Published copies of the policy will be updated to reflect changes but may not be immediately published after updates are approved.

Trust Center