
# Itron Security Center (ISC) Vulnerability Handling Policy

**Revision:** 2.4

**Last Updated:** September 14, 2010

## Reporting a Suspected Security Vulnerability

The Itron Security Center (ISC) is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability-related information, related to Itron products and networks. The on-call ISC team works 24x7 with Itron customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Itron products and networks. Anyone who has a product security issue is strongly encouraged to contact the ISC directly.

## Contacting the ISC

The Itron Security Center team can be reached via e-mail or phone. Please use the information below to contact the ISC for reporting security vulnerabilities or incidents:

Email: secure@itron.com. Reports via e-mail will be acknowledged within 24 hours.

Phone: **1-866-216-2106**. Reports via phone or voicemail will be acknowledged within 24 hours.

**All email submissions containing vulnerability or incident details should be encrypted with the Itron Security Center public key that can be verified at the PGP Global Directory.**

Either contact method is also useful for reporting sensitive data to a limited number of designated Itron security subject matter experts as contacts are limited to Itron employees authorized to manage security incidents.

## Incident Response Eligibility

Customers with service contracts receive incident response assistance for any incident in which an Itron product plays a significant role, regardless of whether there is an identified problem with a Itron product.

All customers, regardless of contract status, may receive free-of-charge incident response assistance for any incident that involves known or reasonably suspected security vulnerability in an Itron product. Itron reserves the right to determine the type and scope of assistance it can offer in connection with any incident and to withdraw from any incident investigation at any time. Itron also may prioritize security incidents that involve actual or potential threats to persons, property, and the Internet, as well as requests from law enforcement agencies or established incident response organizations.

Itron welcomes reports from independent researchers, industry organizations, other vendors, and any other sources concerned with network or application security. The same procedures noted above for reporting product security concerns to Itron should be used.

## The Investigation Process

The ISC investigates all reports regardless of the Itron software code version or product lifecycle status. Issues will be prioritized on the potential severity of the vulnerability and other environmental factors. The ultimate resolution of the reported incident may require upgrades to products that are under active support from Itron.

Throughout the investigation process, the ISC strives to work collaboratively with the source of the report ("incident reporter") in order to confirm the nature of the vulnerability, gather required technical information and ascertain appropriate remedial action. When the initial investigation is complete, results will be delivered to the incident reporter along with a plan for resolution and customer disclosure. If the incident reporter disagrees with the conclusion, ISC will make every effort to address those concerns.

During any investigation, the ISC manages all sensitive information on a highly confidential basis. Internal distribution is limited to those who have a legitimate need to know and can actively assist in the resolution. Similarly, the ISC will ask incident reporters to maintain strict confidentiality until complete resolutions are available for our customers and have been published by the ISC on itron.com via appropriate coordinated disclosure.

For externally reported vulnerabilities, ISC may acknowledge the reporter of the information at their request, in the disclosure of the vulnerability.

For vulnerabilities reported to Itron that may impact multiple vendors (i.e. a generic protocol issue), our practice is to work with third-party coordination centers such as CERT/CC or NISCC to manage a coordinated industry disclosure. In those situations, the ISC will either assist the vulnerability reporter in contacting the coordination center, or may do so on their behalf.

For vulnerabilities reported to the ISC involving another vendor's product(s), the ISC will notify the vendor directly, coordinate with the reporter, or engage a third party coordination center.

ISC will coordinate with the reporter of an incident to determine incident and documentation update frequency and status.

Upon the confirmation of the security vulnerability, the ISC will manage the creation of software patches and/or workarounds to address the vulnerability and subsequent public disclosure. Under the best of circumstances, Itron will publish a mitigation plan when it has a complete set of software patches and workarounds available for customers. In unusual instances such as confirmed active exploitation of the vulnerability or new public information that could increase the risk to customers, Itron will accelerate the publication of a security advisory for the vulnerability. Under these circumstances, accelerated publication may occur in the absence of a complete set of patches or workarounds available. When coordinating disclosure with outside parties, we will attempt to notify them of changes to the ISC public disclosure schedule. A notification email will be sent to the ISC membership for any High or Critical severity rating security advisories issued, and a conference call/and or webcast briefing will be scheduled to coincide with the announcement.

The ISC provides the following types of publications for Itron product security vulnerability information:

- Security Advisories are published for significant security issues that directly involve Itron products and require an upgrade, fix, or other customer action. Security Advisories are posted to the ISC website and automated email alerts for receiving update notifications for any changes made to this document library can be enabled by the user from the Actions menu for the library.
- Issue Reports are published as unofficial notices of possible vulnerabilities. Issue Reports provide a mechanism to share the latest information reported to the Itron Security Center. Issue reports *do not* include a risk assessment matrix and *may not represent real vulnerabilities*.
- Release Control Checks provide cryptographic signatures of release product data files. These signatures can be used to ensure that firmware images and other software provided by Itron are genuine.
- Best Practice Recommendations provide guidance on the best ways to securely use or deploy Itron solutions. Best Practice Recommendations may contain details on hardening the environment for a product, or configuring a product as securely as possible.

**NOTE: Security Advisories and Issue Reports are <u>NOT POSTED</u> to any public mailing lists or newsgroups (for example, BugTraq). Access to these documents requires an ISC approved account, authentication and acceptance of a non-disclosure agreement.**

**ITRON PUBLIC**