GE
Grid Solutions

CyberSentry™ Substation Vulnerability Watch

We monitor so you don't have to.

Rogue actors are actively exploiting vulnerabilities in the products or systems they target making patching and securing endpoints more critical than ever. To protect against these attacks the defense-in-depth strategy requires monitoring of newly published vulnerabilities regularly and taking the right security measures.

Monitoring vulnerabilities for all your products and systems is challenging. This is a never-ending effort of scanning numerous information sources (vendors websites, national vulnerability databases) and mapping the vulnerabilities found to actual substation protection and control systems.

The CyberSentry™ vulnerability watch service takes this burden away from you. A security bulletin listing known vulnerabilities in all substation products, their severity in the context of the substation protection, control and automation and mitigation measures is made available to customers on a monthly basis.

Available software updates are integrated and tested, and impact on the system is described in the security bulletin: 'Compatibility and Mandatory Reboot'.

By implementing proper security update policy, customers can reduce exposure to cyber-attacks and human performance errors during software upgrades. Combining vulnerability detection with security updates testing and on-site deployment provides a full service designed to protect your operations. Where applicable, we can test security updates on your mirrored system to further ensure system integrity.

Key Benefits

- Prevent unplanned downtime and reduced revenues created by successful cyberattacks
- Avoid cyber security compliance fines by passing regulatory compliance audits
- Preserve system integrity by using tested security updates
- Reduced planned downtime by knowing updates which require a reboot and estimated install time

Applications

- NERC CIP compliance
- IEC 62443-2-4 compliance
- BDEW compliance
- Transmission, utilities, industry

Key Features

- Monthly security bulletins
- Event driven security alerts
- Tested security updates
- Digitally signed packaged updates
- Available online
- Deployment by GE or customer

GE Products Security Advisories and Updates

GE PSIRT product security incident and vulnerability management procedures are consistent with ISO 29147 and 30111 for identifying, validating, mitigating, and communicating vulnerabilities in GE products.

Security advisories are available on GE Grid Solutions website.

GE security update packages are digitally signed to ensure integrity.

Patch Compatibility Reports

GE regularly monitors security advisories for third party software that is packaged with GE products, such as operating systems and databases.

Available updates are tested in a controlled environment representing a customer's typical control system to demonstrate that they have no adverse impact on the GE solution.

Findings are summarized in a monthly security bulletin disclosing known vulnerabilities and mitigation measures applicable to the GE solution.

3rd Party Vulnerability Monitoring

Because we deliver turnkey systems that include not just our own products, GE monitors newly published vulnerabilities for the complete protection and control system, according to an agreed inventory.

Each month, a customer tailored bulletin informs on new vulnerabilities for each substation included in the service.

When available, links are provided to third-party security update, maintaining the chain of custody.

GE can deploy the security updates on customer systems as part of its CyberSentry™ Security Services offer.

Additionally, for critical applications, GE can also validate security updates on a customer's mirror platform.

Scope

	Free	**Vulnerability Watch**	
	GE Product	Full Substation	
View GE products security advisories	✓	✓	www.gegridsolutions.com
Subscribe to GE products security advisories	✓	✓	Self-service
Obtain GE software/firmware updates	X	✓	GE products only
Patch compatibility report	X	✓	For 3rd party software packaged with GE products (such as MS Windows 10)
Tailored monthly security bulletins for substation 3rd party products*	X	✓	Monitoring of newly published vulnerabilities for all products installed in the substation including non-GE products.
Updates installed by GE	X	•	Optional
Updates tested on customer's mirror platform	X	•	Optional

** Access to 3rd party security updates are subject to vendors T&Cs*

For more information please contact
GE
Grid Solutions

Worldwide Contact Center

Web: www.GEGridSolutions.com/contact
Phone: +44 (0) 1785 250 070

GEGridSolutions.com