Security Patch Service

fact sheet

GEA-S1291A

The Security Patch Service supports patch management and updated virus signatures, as well as a backup and recovery strategy to support continuity of operations for turbine, generator and plant controls and their associated networks. Customers receive a monthly DVD containing validated and tested patches compatible with existing Human-machine Interfaces (HMIs) and servers. Patch reports detailing US-CERT criticality (if a restart is required) and estimated install time is also provided.

By implementing proper configuration control and a robust patch management plan as well as conducting frequent backups and periodic recovery drills, customers can reduce exposure to cyber attacks and human performance errors during software upgrades. Ongoing system hardening reviews as a due-diligence process against GE's list of ports and services during the cyber vulnerability assessment cycles are highly recommended.

Benefits

- Proactive and timely monitoring of software security patches and antivirus malware signatures using a centralized patch deployment tool
- Predefined checklist to verify proper control system functioning, and meet regulatory requirements for adequate patch testing to prevent potential adverse effect
- Database containing the status of antivirus signatures installed on the HMIs
- Inventory of machines and history of security-related patches applied to specific machines on the security server
- HMI restart status, patch status, vulnerability assessment, and patch management plan trends for compliance audit-ready reports

Applicability Evaluation and Status Reporting

GE reviews security updates and antivirus signatures released for their applicability on GE-provided HMIs and servers. Based on this review, a candidate list of patches and updates is then tested. Each DVD provides cumulative updates (systems are updated to the latest revision even if a previous DVD was not applied). GE provides both a monthly record of updates applicable to a specific system and the status of the update (applied or missing). This report can be used to support audit activities pertaining to patch management.

Testing

GE maintains a validation laboratory where Windows 7, application patches, and antivirus/host intrusion detection signature updates are tested in a controlled, representative environment simulating the customer control system.

Testing demonstrates that functional operation of the control and related interfaces, as well as communication to the system is not adversely impacted by the patches. Any patches identified that could potentially impact operations are excluded.

Packaging and Secure Delivery

TPatches are assembled into a single package that an operator can manually install on each HMI. They can also be used through the optional SecurityST Cyber Security Management System (CSMS). Whether at the host or network level, any update actions must be initiated by the operator prior to use.

The patches are delivered to the site through securely sealed and tamper-evident shipping envelopes. The chain of custody for the update is also maintained throughout transit to the site.

Ports and Services

GE provides an ongoing updated list of ports, services, and programs on the HMIs. This allows the end user to document and track services, programs, drivers, and ports in use, or installed on the HMI computer for normal and emergency services. This information can be used to further refine and manage these components.

Backup and Recovery

GE provides software for both backup and automated recovery of backup to support disaster recovery policies and practices.

The GE solution assists the customer in enforcing change management and implementing frequent backups of evidence to demonstrate compliance status.

The SecurityST server database keeps an inventory of HMIs and the history of security-related patches applied to those HMIs. The status of antivirus signatures installed on the HMIs is also kept in the database.

Backups are performed and stored on the SecurityST server. It is configured to store a maximum of one year's backups for up to 10 HMIs.

Security Information and Event Management

The Security Information and Event Manager can create an event, alert, and alarm when changes are made to ports and services, operation system versions, software, and patch levels. It also provides reports for:

- Electronic access points of firewalls
- Computers
- Servers
- Intrusion detection and protection system sensors
- Virtual devices

The SIEM supports logical grouping of assets. This can organize assets by function, type, operating system, or other attributes for compliance reporting of general overviews and in-depth reviews based on event types. The easily customizable report engine can generate unit-specific reports, export data to a .csv file, and tab limited format.

Event logs from all Windows HMIs in the Integrated Control System (ICS) are stored. The SIEM also stores security events created on network equipment, such as logon and logoff events and configuration changes. This information is stored and backed up.

GE is positioned to assist customers in conducting timely testing as well as applying critical software security patches. Customers are advised to have effective configuration control procedures that include evaluation, approval, and management of change.

For further assistance or technical information, contact the nearest GE Sales or Service Office, or an authorized GE Sales Representative.

GEA-S1291A Issued: Mar 2013 Revised: Sep 2014