



PATCH BINARY ACQUISITION

OVERVIEW

Industrial Control Systems (ICS) in critical infrastructure continue to be considered high-risk targets for attack and exploitation. Just as with typical home PCs and business computing platforms, cybersecurity vulnerabilities in these ICS environments are ever being discovered and exploited by malicious actors. The application of security patches to systems in those environments is one way to reduce risk and mitigate the vulnerability. Patch management in complex ICS environments requires a comprehensive approach designed to support the specific needs of these types of systems. Patch acquisition can be a challenge when assets, segmented from the internet, are included. Automation tools cannot be used to simplify the downloading and acquisition of patches from ICS vendors. Individual manual downloads may be required, which can often introduce additional cyber risk. How do you ensure patches are from legitimate sources? How do you ensure downloaded patches are authentic and not compromised? Those responsible for the patching of systems and equipment in an ICS environment must overcome these challenges. A robust set of procedures and processes to securely acquire each patch is required.

FoxGuard offers a service to help. Our Patch Binary Acquisition service can significantly simplify your patch management program.

During the acquisition process, we have the ability to securely download your required patch binary files.

PATCH BINARY ACQUISITION PROCESS

When you add this service to your patch management program, your FoxGuard team will:

- Download your patch binary files
- Document and verify the *integrity* of your patch binary files by hash comparison
- Document the *authenticity* of your patch binary source utilizing cryptographic methods
- Perform anti-malware scanning on all patch binary files
- Package all binary files using FoxGuard's proprietary hashing tool to insure a secure supply chain delivery via encrypted distribution

We have established strong vendor partnerships, making the process of gathering patch information and downloading required patches efficient, saving you time and labor.



BENEFITS

- NERC CIP-007, CIP-010 AND CIP-013 COMPLIANCE
- LABOR COST REDUCTION
- THIRD PARTY TOOL INTEGRATION SUPPORT



RELATED PRODUCTS

- PATCH AVAILABILITY REPORT
- SENTRIGARD PATCH DEPLOYMENT CONSOLE
- BASELINE & PATCH SERVICES

KEY PROGRAM FEATURES

EVERY PATCH BINARY ACQUISITION DELIVERY CONTAINS THE FOLLOWING SECURITY CONTROLS:

Vendor Integrity Verification: Where the software vendors provide cryptographic hash values associated with the patch binary file(s) to be downloaded, FoxGuard will verify that the files downloaded from the vendor's website yield the same cryptographic hash value as a means to verify patch file integrity.

Vendor Authenticity Verification: For patch binary files that are digitally signed, FoxGuard will review downloaded patch binary files for certificate / digital signature signing status as a means to verify patch file authenticity.

Digital Tampering Protections: FoxGuard digitally signs every deliverable for verification by the customer, using the FoxGuard Hash Comparison Tool. This tool is provided prior to the initial patch binary file deliverable, and allows customers to verify the integrity and authenticity of the files received from FoxGuard each month.

Vendor Credentials: Secure management of your vendor credentials required during the mining process.

Secure Media: The monthly distribution is delivered to site on an encrypted USB drive. All data on the drive is encrypted and locked by a customer specific password.

Tamper Resistant Packaging: Every delivery comes sealed in tamper resistant packaging.

Providing
**PATCH
MANAGEMENT
SERVICES**

OVER **1000**

Sites
World-wide

WHY FOXGUARD



EXPERIENCE

FoxGuard has over 15 years of experience creating secure comprehensive patching solutions. We know the industry's assets because we have analyzed, documented, and verified patch details for these assets for years.



INDUSTRY LEADER

The company was founded in 1981, in Christiansburg, Virginia. We have the experience and in-depth knowledge to support patch management programs in critical infrastructure. In 2014 we partnered with the Department of Energy (DOE) to develop a patch management for the energy utility industry. FoxGuard works with several leading energy equipment OEMs and directly with electric utilities; supplying patch management and cybersecurity solutions globally.



AUDIT SUCCESS

Our customers are world wide and FoxGuard is proud to say that 100's of our customers have successfully passed regulatory and security audits.



FoxGuard Solutions® is a wholly owned subsidiary of Framatome, an international leader in nuclear energy.



www.foxguardsolutions.com



requestinfo@foxguardsolutions.com



877.446.4732