framatome cybersecurity

PATCH BINARY ACQUISITION

Simplify and enhance Patch Management with Patch Binary Acquisition (PBA) solution

The one-stop-shop for seamlessly and securely acquiring all your patch binaries.

Challenge

Patch management is critical for protecting critical systems from cyberattacks. However, it could be challenging and time-consuming to identify, acquire, and verify the authenticity and integrity of patches, especially nowadays most systems contain thousands of assets from multiple vendors.

Furthermore, the need to prevent compromise and ensure patch reliability further complicates the patch acquisition process.

Solution

Framatome's Patch Binary Acquisition (PBA) service is designed to simplify and secure your patch acquisition process. When you incorporate our service into your patch management program, our experts offer the following benefits:

- Downloading your required patch binary files securely.
- Documenting and verifying the integrity of patch binary files using hash comparison techniques.
- Authenticating the source of patch binary files through cryptographic methods.
- Conducting anti-malware scanning on all patch binary files.
- Packaging all binary files using Framatome's proprietary hashing tool to ensure a secure supply chain delivery with signed encrypted distribution.

Customer benefits

- **Achieving an up-to-date and secure environment:** By regularly patching vulnerabilities, you effectively manage and reduce the risk of attacks.

- **Securing supply chain for software acquisition:** We help you secure your supply chain by certifying the source and version of security patches. Our expertise ensures protection against malwares or unreliable patch sources. Additionally, we provide non-security patches.

Your performance
is **our** everyday **commitment**

@ EDF

Technical information

- **Vendor integrity verification:** We rigorously verify the integrity of patch files downloaded from vendor websites to ensure their reliability.
- **Vendor authenticity verification:** For digitally signed patch binary files, we review and validate their authenticity.
- **Digital tampering protections:** Every deliverable is digitally signed and provided for verification using our Hash Comparison Tool, ensuring tamper-proof distribution.
- **Vendor credentials:** We securely manage your vendor credentials required during the patch mining process.
- **Secure media delivery:** Deliverables are provided via a carrier-grade, secure portal for confidentiality and integrity.

Key figures

70% of OT cybersecurity professionals believe that their organization is at high risk.
OT Security: The State of Play, by SecurityScorecard

The average cost of an OT cyberattack is

$3.7 million.
The Cost of Cyberattacks on Industrial Control Systems by Ponemon Institute.

Contact: cyber-services@framatome.com
www.framatomecybersecurity.com