FOXGUARD SOLUTIONS®

PATCH AVAILABILITY REPORT

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 frequently being discovered and exploited by malicious actors. The application of security patches to systems in those environments is one way to mitigate the vulnerability, reduce risk, and increase reliability.

Patch management within ICS environments requires a comprehensive approach designed to support the specific needs of these types of systems. Many different vendors and asset types can make patch management a challenge. Automation tools are not typically successful to quickly determine what patches and software updates are available for the devices in your environments. Tedious, manual research is often required to determine whether a vendor has released patches for software running in your environment. Knowing where to go to find all of the information can often pose a challenge as well. How do you ensure you are researching patch availability from legitimate sources? How do you ensure you have gathered all of the information necessary to support further analysis and decision making on whether available patches are actually applicable to your environment? Those responsible for the patching of systems and equipment in the ICS environment must overcome these challenges. A robust set of procedures and processes during this initial research and documentation phase is required to ensure success of downstream patch management activities. Consistently monitoring for the release of software patches and updates can lead to improved security awareness, leading to an overall reduction of cyber risk. Downstream application of patches can mitigate security vulnerabilities, address functional issues, and with meeting regulatory compliance requirements.

Expense incurred to support the continual research and documentation of all security patches for all critical assets is an often overlooked, and often costly element of a comprehensive patch management program for any Industrial Control System. This task alone can be daunting and extremely time-consuming, usually performed by highly compensated engineers who are responsible for other critical work. Vendors often manage their patch releases differently. Not all vendors provide security classification for their patches. Economies of scale may be challenging to realize, given the variety of ICS equipment that may be present in your environment.

BENEFITS

ONE SOURCE • ONE CALENDAR

AUDIT READY

SECURITY CLASSIFICATION • SECURITY PRIORITIZATION

LIFECYCLE MANAGEMENT

THIRD-PARTY INTEGRATIONS

RELATED PRODUCTS

PATCH BINARY ACQUISITION

SENTRIGARD PATCH DEPLOYMENT CONSOLE

VULNERABILITY NOTIFICATION REPORTING

PATCH VALIDATION SERVICES

ASSET ID & BASELINE CONSULTATIVE SERVICES

SOLUTION

To ease the burden of patch research and availability determination, FoxGuard offers its Patch Availability Reporting (PAR) service. Every 30 days, we will provide you with a detailed intelligence report customized to your hardware and software asset list. This report provides all of the security patch information needed to drive your patch management program to success. We take on the responsibility of monitoring all of your software vendors for the release of new security patches and firmware updates, so that you can focus on other business needs. Reports provide patch information at both a high-level summary (for quick review) as well as a detailed list of attributes (for operational execution). We include information such as: when a vendor has released a security patch for an asset we are monitoring for you, whether the asset is still supported by the vendor, associated vulnerability information, security classification and security summary notes, as well as patch download links, vendor-supplied cryptographic hash values of the patch file, vendor notes and other pertinent details required for a thorough assessment. Reports are available in human-readable and machine-readable formats to allow the interaction of intelligence data with your existing systems. Compliance evidence is also made available for each asset, assisting in process verification or audit support efforts.

Optionally, our ICS Update Patch Visualization Engine allows you to visualize your patch data via an intuitive, easy to use dashboard. Use it to bring the most important details about your assets and available patches, to the surface. ICS Update allows users to understand the number of patches available per asset to simplify the identification of which assets you should focus on first and to know which patches address the most critical security vulnerabilities.

OUR APPROACH: ONE REPORT. ONE SOURCE. ONE CALENDAR.

For customers in the electric utility sector looking to simplify the patch management processes in support of NERC CIP standards, we offer our PAR service as a way to support your NERC CIP-007 R2 source identification needs and to streamline availability determination efforts. We take on the burden to contact vendors and research vendor websites for available patches. You can benefit from the identification of single-source, operating against a single 35-day patch cycle clock, and simplify the management of many sources and compliance workflows that you may have needed previously. Our PAR service offering will remove countless hours of phone calls, web scraping, spreadsheet updates, and writing e-mails to vendors, all in support of determining whether the vendor has released a patch for each of your assets. You can now focus on your business priorities and let FoxGuard do what we do best.

Provide us your list of assets, and we'll take it from there. Our team of engineers will engage in an in-depth review of your asset list and will evaluate it against our patch and vulnerability intelligence data warehouse.* Our program supports many different software types, including BIOS / UEFI software, device firmware, operating systems, drivers, software applications, controls software, and more. We support software from over 450 different vendors and continue to grow the list of those we support. If we currently do not work with a specific product or vendor, we will work with you to add them to our program.

** We understand the asset data you provide to us includes sensitive information – we take the protection of that data seriously. We will be happy to discuss how we keep your information safe and secure, helping you meet NERC CIP-013-1 and similar regulations.*

SOLUTION OFFERINGS

FoxGuard offers two unique
patch availability reporting solutions.

TRADITIONAL PAR:

Our Traditional PAR offering designed for customers in need of a Security Patch Report for a relatively static asset list with minimal change to the assets within the environment. Simply provide us the list of software you want us to monitor, and we will provide monthly reports on that list. Workflows exist to support modifications to the monitored software list as your asset list evolves.

DYNAMIC PAR:

Let us track asset changes for you. Under Dynamic PAR, we can help you maintain up-to-date asset lists for your environment. We will review your asset list each time we receive it and will provide a monthly Security Patch Report, accounting for the changes detected. Under this program, we will adjust your report to support all changes to your asset list.

ATTRIBUTES	FEATURES	TRADITIONAL PAR	DYNAMIC PAR
Core Features	Monthly PAR Report	●	●
	Alternative Report Schedule	Optional	Optional
	CIP-007 R2 Support	●	●
	CIP-010 R1.6 Support	●	●
	EOS/EOL Notification	●	●
	EOS/EOL Documentation	●	●
	Links to Patch Binary Files & Release Notes	●	●
	National Vulnerability Database (NVD) Intelligence	●	●
	Documentation of Vendor and FoxGuard Release Dates	●	●
	On-Demand Access to Compliance Evidence Documentation	●	●
	Security Patch Analysis	●	●
	Secure Report Download	●	●
	ICS Update Patch Visualization Engine	Optional	Optional
Asset Support	Microsoft Windows Operating Systems	●	●
	Microsoft Software (Non OS)	●	●
	3rd Party Software	●	●
	Driver / BIOS Support	●	●
	Network Devices	●	●
	ICS Vendor Approved Patches at Device Level	●	●
	ICS Device Firmware & Software	●	●
	Field Devices	●	●
	Red Hat Enterprise Linux - 6.x, 7.x, 8.x	Optional, Partial	❍
	CentOS - 6.x, 7.x, 8.x	Optional, Partial	❍
Report Type	Master Asset (One-to-One Mapping with Customer Supplied Data)	Optional	Optional
	Unique Items (Non-Duplicated Data)	Optional	Optional
	Cyber Asset Identifier (Non-Duplicated Data Grouped by Customer Specified Asset)	Optional	Optional
Report Formats	PDF (Human Readable)	●	●
	HTML (Human Readable)	Partial, Linux Only	Partial, Linux Only
	JSON (Optimized for Data Integrations)	●	●
	CSV (Human Readable, Can be Used for Data Integrations)	●	●
Other	Static Asset List	●	❍
	Dynamic Asset List	❍	●
	One-Way Integration Ready	●	●
	Two-Way Integration Ready	●	●

KEY PROGRAM FEATURES

NERC CIP Audit Ready: Need to meet regulatory audit requirements like NERC CIP-007? Our PAR offering has been utilized by electric utility customers to successfully meet security and regulatory requirements in all NERC regions throughout the U.S. and Canada. We include all of the details needed in our reports and back that up with the necessary evidence (available for download on-demand), to support audit requirements.

One Source: FoxGuard aggregates all of your assets and vendors into one source – eliminating the need for you to contact and follow up with all of your vendors every month. *FoxGuard is your one source.*

Save Valuable Time: This work can be complicated and require significant technical resource investment to address the intricacies involved. Save the time of your valuable resources to focus on your business and leave the patch management work to us.

Security Classification: Our trained engineers analyze patch details to determine if a patch addresses a security vulnerability, even if the patch vendor doesn't make this declaration. This analysis allows you to prioritize the patches that are needed to secure your critical systems.

Security Prioritization: Your time is limited, and we understand that it may be weeks or months before your ICS systems become available for patch installation. Use the data included in our PAR reports along with the ICS Update Patch Visualization Engine to prioritize where to focus your time. Identify those patches with the most significant vulnerability impact.

Lifecycle Management: Not every product lives forever. When a vendor no longer provides patches for an asset, you need documentation to show why you are no longer monitoring it for patches. We provide end of life confirmation documentation. We've got that covered.

Third-Party Integrations: Have some form of an automated Asset Management System or Compliance Tool? We can work with your vendor to automatically integrate our reports into your system, automating the process of importing newly released patches.

One Calendar: Because you have only one source, your compliance calendar of 35 days for the subsequent NERC CIP-007-6 R2.1, R2.2, R2.3 and R2.4 requirements stops and starts at the same time. Just one calendar to manage instead of potentially hundreds of vendors. Every month.

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 provide patch management programs to critical infrastructure. In 2014 we partnered with the US Department of Energy (DOE) to develop a patch management program 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 hundreds of our customers have successfully passed regulatory and security audits.

www.foxguardsolutions.com
requestinfo@foxguardsolutions.com
877.446.4732