



# VULNERABILITY NOTIFICATION REPORT

## OVERVIEW

Industrial Control Systems in critical infrastructure are continuing to be considered high-risk targets for attack and exploitation. Consistently monitored patches and updates can help resolve security vulnerabilities, functional issues and meet regulatory compliance requirements. Compliance programs like NERC CIP-007, NEI 08-09, NIST CSF, TS 50701, US DOD CMMC require you to create a comprehensive security program to manage the risk to your control systems by implementing solid security practices and cyber solutions. One of the biggest challenges to managing a good security solution involves gaining a solid understanding of actual risk on the network.

## SOLUTION

Provide a list of assets and we'll take it from there. Our team of engineers will implement an in-depth analysis of your list to onboard your assets into our secure and anonymized patch and vulnerability data warehouse. Our program supports most any software found in your control system including OS, drivers, BIOS, 3rd party software, controls software, network devices, and field devices. If we currently do not work with that product or vendor, we will work with you to add them to our program.

We utilize the National Vulnerability Database, the U.S. government's repository of standards-based vulnerability management data represented using the Security Content Automation Protocol, to extend our patch intelligence to include a more comprehensive risk report. This data enables automation of vulnerability management, security measurement, and compliance. By downloading the national vulnerability database nightly and incorporating it into our database, we are able to search and correlate new vulnerabilities in a customer's environment. With

this offering, FoxGuard Solutions has solved the problem of offline vulnerability scanning. This also eliminates the risk of taking a device offline while running traditional scanning technologies.

This offering can be incorporated into a new or existing vulnerability management program, enabling our customers to have better control and visibility of their overall risk. By purchasing Vulnerability Notification Report (VNR), our customers have the tools to prioritize risks and remediation tactics without the threat of service interruption in their environments.

Every 30 days you will receive our Patch Vulnerability Report detailing all publicly known information needed to support the risk assessment of your network. Each report will detail every asset under your program, End of Life information, and CVE information. Each report can be made available in human readable and machine-readable formats.

As a services extension to our Patch Availability Report (PAR), your monthly Vulnerability Report will give you a comprehensive understanding of all known vulnerabilities in your environment and patch and update details, when available, to address each vulnerability.



## BENEFITS

ALIGNS WITH PATCH AVAILABILITY REPORT (PAR)

COMPREHENSIVE VULNERABILITY REPORT

ALIGNS TO YOUR ASSET ENVIRONMENT

FoxGuard's Vulnerability Notification Report (VNR) service extends the Patch Availability Report (PAR) intelligence service to give you a more comprehensive understanding your risk profile. Combined, these two services give you a single sourced monthly risk review or every asset specific to your environment. You will save countless hours scouring the internet to locate patch and vulnerability risk details, freeing your team to focus on what is most important.

#### FEATURES INCLUDE:

1. CVSS v2 and CVSS v3 support
2. Comes in machine readable and human readable formats
3. Can integrate into currently deployed vulnerability management programs

### KEY PROGRAM FEATURES

**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 contact.

**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 work to us.

**Understand your risk:** To fully understand your cyber risk, it is important to be aware of vulnerabilities that may or may not have had a patch released by the vendor. Patch Availability Report (PAR) alone does not give you the complete picture. By adding VNR to your program you will have both the patch and vulnerability information enabling you to better protect your critical assets.

**End of Life** Not every product lives forever. When a vendor no longer provides patches for that software asset, you need documentation to show why you are no longer monitoring it for patches. We've got that covered.

### WHY FOXGUARD



#### EXPERIENCE

FoxGuard has over 15 years of experience creating secure comprehensive patch and risk management 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 the last few years we partnered with the Department of Energy (DOE) to develop a simplified patch management program for the energy utility industry. FoxGuard works with several leading 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 security and regulatory audits, while leveraging our products and solutions to support their compliance needs.

**framatome**

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



[www.foxguardsolutions.com](http://www.foxguardsolutions.com)



[requestinfo@foxguardsolutions.com](mailto:requestinfo@foxguardsolutions.com)



877.446.4732