

# Software Supply Chain Risks and Mitigations for NERC CIP-010-3 R1, 1.6

August 12, 2020

Presented by: Energy Central

Thank you to our sponsor

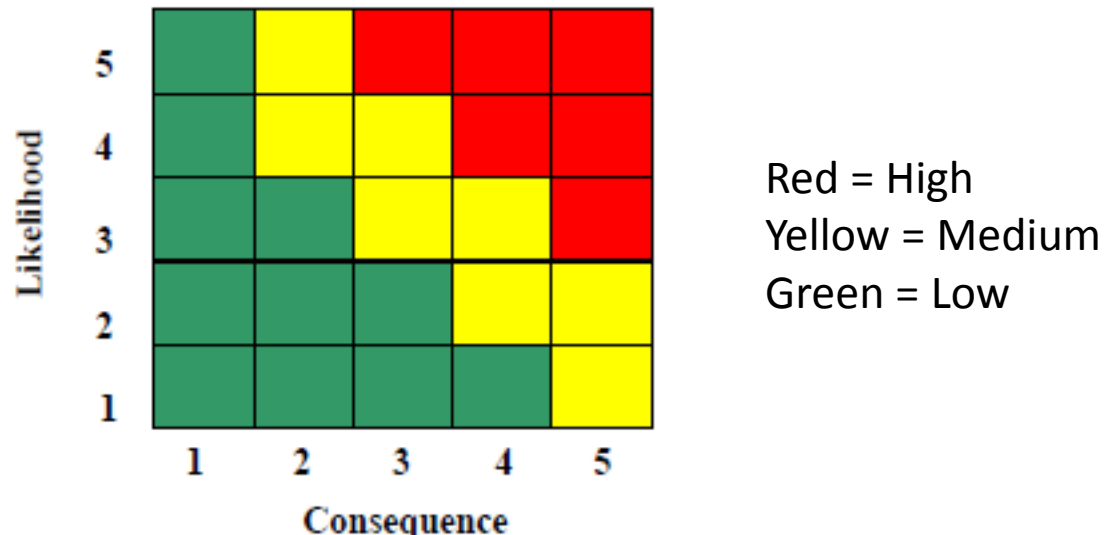


# Topics

- Software Supply Chain Risks and Threats
- Software Risks
- Value at Risk
- Risk Assessment Steps for NERC CIP-010-3 1.6
- Constant improvement is **REQUIRED**
- Summary

# Definition of Risk

- The Department of Defense (DOD) Office for the Undersecretary of Defense for Acquisition defines risk as **Risk = Likelihood x Consequence of a “future root cause (yet to happen), which if eliminated or corrected, would prevent a potential consequence from occurring” (OSD/ATL-ED, 2006).**



# Definition of Threats

- Real tactics, techniques and procedures (TTP) that are proven to successfully carry out a cyber attack, by parties at various skill levels with the intent, capability and opportunity to do so.
- Some threats are known, some are not (i.e. 0-day exploits)

## **Explanation of the Current Alert Level of GUARDED**

**The alert level is the overall current threat level.**

Read more about our approach. →

On May 20, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Palo Alto, PHP and Google products. On May 15, the MS-ISAC released an advisory for multiple vulnerabilities in Palo Alto PAN-OS, the most severe of which could allow for session fixation attacks. On May 18, the MS-ISAC released an advisory for multiple vulnerabilities in in PHP, the most severe of which could allow for denial of service conditions. On May 19, the MS-ISAC released an advisory for multiple vulnerabilities in Google Chrome, the most severe of which could allow for arbitrary code execution. Organizations and users are advised to update and apply all appropriate vendor security patches to vulnerable systems and to continue to update their antivirus signatures daily. Another line of defense includes user awareness training regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

<https://www.cisecurity.org/cybersecurity-threats/>

# Providing Context

**ID.RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk

NIST Cybersecurity Framework V1.1

<https://doi.org/10.6028/NIST.CSWP.04162018>

A ***threat actor*** carrying out a ***threat action*** by exploiting a ***vulnerability*** resulting in a ***Consequence*** that causes an ***impact*** in the production process.

Sinclair Koelemij

<https://otcybersecurity.blog/2020/06/17/consequence-with-capital-c/>

June 17, 2020

**Key Concept:**

**The higher the risk, the lower the trust; Increased risks negatively impact trustworthiness**

# Software Supply Chain Risks

- Risks that exist when acquiring a software object via an Internet Download
  - Spoofed download sites: <http://downloads.Microsoft.com>
  - Watering holes
  - Man in the middle attacks
  - Open Source binary distributions
  - Fakes
  - [Equifax](#) blamed its breach on a flaw in outside software it was using. It then blamed a **malicious download link on its website to yet another vendor.**
- Software/Supplier Risks
  - Third Party software embedded in a Vendor offering
  - Embedded open source software within a vendor product
- A software vendor may not be aware they have been hacked and are distributing tainted software to their customers:
  - [ASUS](#) March 29, 2019
  - [Sophos Threat Report 2020](#)



## Common Types of Malware

@Hackercombat



### Virus

Spreads with your action



### Trojan

Disguised as legitimate software



### Worms

Spreads automatically



### Spyware

Monitors your activity



### Rootkit

Hides deep within your computer



### Adware

Maliciously serves you ads



### Exploit Kit

Hunts software vulnerabilities



### Ransomware

Blocks access to your files/ computer

@Hackercombat



# NERC Supply Chain Risk Alert

[Home](#) > [Program Areas & Departments](#) > [Reliability Risk Management](#) > [Bulk Power System Awareness](#) > [Bulk Power System Awareness](#) > [Alerts](#)

## Alerts

To acknowledge, respond to, or approve of an alert, please [click here](#).

### Alerts

Date	Description	Responsible Entities
☰ 2020 Alerts (2)	<b>Industry Recommendation:</b> Supply Chain Risk - III	Balancing Authority, Distribution Provider, Distribution Provider-UFLS, Frequency Response Sharing Group, Generator Owner, Generator Operator, Planning Authority, Reliability Coordinator, Resource Planner, Regulation Reserve Sharing Group, Reserve Sharing Group, Transmission Owner, Transmission Operator, Transmission Planner, Transmission Service Provider

## ZDNet Security

July 1, 2020

# Ransomware is now your biggest online security nightmare. And it's about to get worse



# Breaking trust: Shades of crisis across an insecure software supply chain

Software supply chain security remains an under-appreciated domain of national security policymaking. Working to improve the security of software supporting private sector enterprise as well as sensitive Defense and Intelligence organizations requires more coherent policy response together industry and open source communities. This report profiles 115 attacks and disclosures against the software supply chain from the past decade to highlight the need for action and presents recommendations to both raise the cost of these attacks and limit their harm.

# Key Trends

- **Deep Impact from State Actors:** There were *at least 27 different state attacks* against the software supply chain
- **Abusing Trust in Code Signing:** These attacks undermine public key cryptography and certificates used to ensure the integrity of code
- **Hijacking Software Updates:** **27% of these attacks targeted software updates** to insert malicious code against sometimes **millions of targets**
- **Poisoning Open-Source Code:** These incidents saw attackers either modify open-source code by gaining account access or post their own packages with names similar to common examples
- **Targeting App Stores:** **22% of these attacks targeted app stores** like the Google Play Store, Apple's App Store, and other third-party app hubs to spread malware

# CIP-010-3 NERC Guidance

- The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software.
- Processes or procedural controls that require users to obtain software directly from the developer or vendor's preferred delivery methods.
- A Responsible Entity may demonstrate compliance with CIP-010-3 R1, Part 1.6 by using processes for software updates that technically enforce that only digitally signed software is installed.
  - This guidance could lead to some really bad outcomes!
  - See Common Misconceptions later in the presentation to see why.

# FERC White Paper and NIST CSF

- [NIST Cybersecurity Framework V1.1, April 2018](#)
- [FERC Cybersecurity White Paper 6/18/2020](#)
- NIST CSF, a framework to implement best practices
- FERC WP, suggests that NIST CSF may be appropriate for “cybersecurity best practices” in the Bulk Electric System
- The software risk assessment approach described in this webinar follows the NIST CSF Identify function (ID.RA, ID.RM and ID.SC) and Protect function PR.DS-6
- The risk assessment approach described in this session may serve as an example of a cybersecurity control that could be eligible for additional incentive compensation (2%), if FERC proceeds with it’s proposal in the white paper

# Evaluating Risk and Establishing Trust Triangulating Corroborating Evidence

Software SBOM/Digital Signature



**TRUST**

Vendor supplied data\*

Ground Truth/Vulnerabilities

# Questions?

Dick Brooks

[dick@reliableenergyanalytics.com](mailto:dick@reliableenergyanalytics.com)



# Software Risks

- Risks inherent in a software object, regardless of where it was acquired
  - Embedded malware (i.e. RATs, Ransomware, mining, worms, etc.)
  - Vulnerabilities and Exploits
  - Fakes
  - Backdoors
  - Third Party embedded objects (Open Source)
  - External Dependencies, i.e. WEB API's
  - Others, yet to be discovered (inevitable)

# Value at Risk

- Understanding the risk associated with your supply chain is key to ensuring security measures and mitigations are proportionate, effective and responsive
- Credit Rating Agencies beginning to factor-in cybersecurity controls in GRC assessments, i.e. [Moody's/Team8 Cyber Assessments startup](#)
- Board of Directors and Executives care deeply about credit ratings!
- Cost of a breach: \$730k – \$1.4M
  - [Norsk Hydro](#), estimated at \$64 - 76M
  - [MAERSK](#) Not Petya attack: \$200-300M

# Cyber Insurance Realities

It wasn't enough. Some 35,000 employees were locked out of the company's network, and Hydro had to shut down several manufacturing plants in Europe and the U.S. The ones still operating had to figure out how to do so without any computers. In the end, the attack would cost the company more than \$60 million—way more than the \$3.6 million the insurance policy has paid out so far, according to an earnings report. It was, according to the prosecutor investigating the breach, the worst cyberattack in Norway's history.

<https://www.bloomberg.com/news/features/2020-07-23/how-to-survive-ransomware-attack-without-paying-ransom>

# Software Risk Assessment Steps

1. Perform introspection of software object looking for risk
2. Verify Download Server Source Location/Certificate
3. Perform Virus Scan for known malware
4. Verify Digital Signature of software object
5. Perform Vulnerability (CVE) Search
6. Perform Vendor Verification using available data
7. Perform Man in the Middle Check
8. Generate a Trustworthiness Score based on risk assessment
9. Save all findings and results in an evidence file

# Software introspection

- After acquiring a software object, perform a deep inspection
  - Create a software [Bill of Materials \(SBOM\)](#) and investigate each potentially dangerous component searching for risk
  - Akin to an FDA food label listing ingredients contained in a food product
  - Identify the Manufacturer/Developer of the SW
  - Determine the name of the product associated with the software along with the version
  - Verify that the developer and product information match the information acquired during procurement discussions with the vendor, [refer to EEI model](#)

# What is an SBOM (NTIA Definition)

## What is a Software Bill of Materials?

An SBOM is effectively a nested inventory: a list of ingredients that make up software components. An SBOM identifies and lists software components, information about those components, and the supply chain relationships between them.

Baseline Software Component Information
Supplier Name
Component Name
Unique Identifier
Version String
Component Hash
Relationship
Author Name

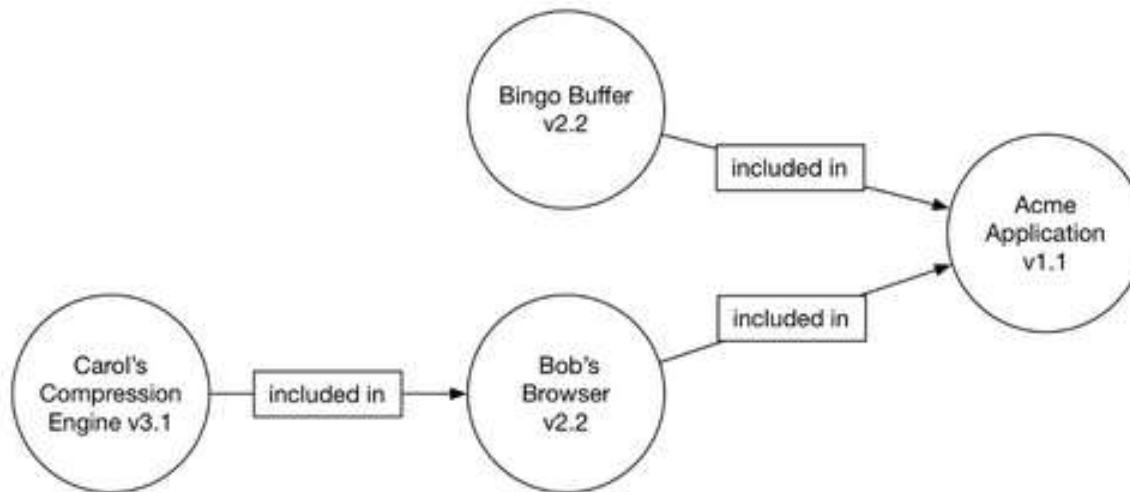


Figure 1: The baseline SBOM includes components in their assembled relationship. Each component has enough information to “uniquely and unambiguously identify” it (left), and the relationship of what upstream or child components are “included in” downstream or parent components (right).<sup>2</sup>

# Verify Source Location/Vendor

- Parse the SSL digital certificate for identification information; is the issuing CA performing thorough investigations of identity before issuing the certificate
- NAESB Accredited CA's offer the best protection; require your software vendor to acquire their digital signing and SSL/TLS certificates from a [NAESB ACA](#), such as Globalsign
- Verify the validity of the digital certificate
- Confirm that the vendor and source location information match what was agreed to during procurement discussions
- Source Locations that lack SSL digital certificates should never be trusted

# Be selective when choosing a CA

{\* SECURITY \*}

**Digicert will shovel some 50,000 EV HTTPS certificates into the furnace this Saturday after audit bungle**

You've got less than 42 hours to regenerate your certs

Fri 10 Jul 2020 // 00:29 UTC

37  GOT TIPS?

[https://www.theregister.com/2020/07/10/digicert\\_pulls\\_certs/](https://www.theregister.com/2020/07/10/digicert_pulls_certs/)



# Malware and Vulnerabilities

- Malware is a deliberate attempt by a hacker to implant software in a victims computing ecosystem in order to gain a foothold to perform nefarious acts, Examples:
  - Not Petya
  - WannaCry
  - Too many to list...
- Vulnerabilities are unintentional software imperfections which a hacker uses to access a victims computing ecosystem, using known exploits, in order to gain a foothold to perform nefarious acts.
  - OS/soft PI vulnerabilities advisory from CISA: <https://www.us-cert.gov/ics/advisories/icsa-20-133-02>
  - Palo Alto Networks vulnerabilities from NIST: <https://nvd.nist.gov/vuln/detail/CVE-2020-2018>
- Vulnerability exploits are often used to implant malware; They are not mutually exclusive risks

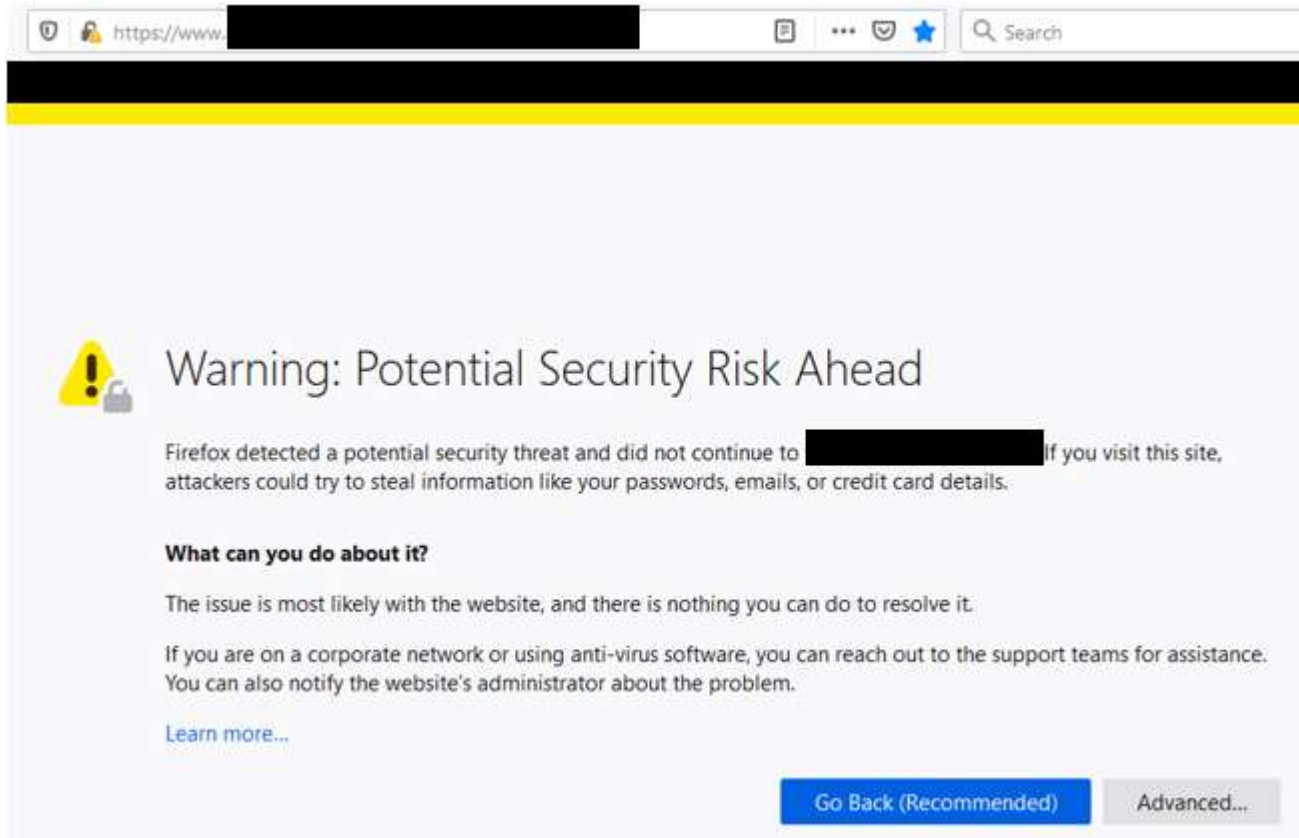
# Malware and Vulnerabilities

- Perform a malware scan using trusted and up to date antivirus software; any discovered malware automatically results in a trust score of ZERO
- Perform a search for known vulnerabilities and exploits
  - Signup to receive CISA alerts and advisories
  - Search known vulnerability databases, i.e. Mitre CVE and NIST NVD
  - I've proposed changes to [Rapid7 to improve AttackerKB](#) search results
- Any discovered malware or vulnerability risks results in a trust score of ZERO

# Software Object Provenance

- Look for man in the middle risks, i.e. Blacklisted IP addresses and foreign risks
- Examine a digital signature, if present:
  - Look for any indication of expired certificates
  - Look for “freshness” of the digital certificate, if it’s too old then it may not be trustworthy; check timestamps
  - Verify digital signature information with data acquired during procurement discussions and contract signing
- Lack of a digital certificate reduces trust to zero
- A matching hash value will improve the integrity score, but offers no assurance for identity/authentication

# Real Experiences; Bad SSL Cert



# Untrustworthy SSL/TLS Certs

- Let's Encrypt
- Let's Encrypt issued 3,048,289 TLS certificates without checking the CAA field for the requesting domain.
- <https://www.zdnet.com/article/lets-encrypt-to-revoke-3-million-certificates-on-march-4-due-to-bug/>

# Embedded Malware

```
Performing Malware Scan(this takes a few moments...)  
(---->Engine: ESET-NOD32', 'result:', True, 'reason:', 'a variant of Win64/WinDivert.A potentially unsafe')  
(---->Engine: Emsisoft', 'result:', True, 'reason:', 'Application.WinDivert.B (B)')  
(---->Engine: Fortinet', 'result:', True, 'reason:', 'Adware/WinDivert')  
(---->Engine: Qihoo-360', 'result:', True, 'reason:', 'Generic/Application.918')  
---->Vulnerabilities found: 4 Total Scans performed: 42  
A trust score of: 0 has been calculated for this step. Do you wish to assign a passing grade (Y)/N?
```

```
Performing Malware Scan(this takes a few moments...)  
(---->Engine: ClamAV', 'result:', True, 'reason:', 'Win.Trojan.Agent-7477406-0')  
---->Vulnerabilities found: 1 Total Scans performed: 73
```

# Digital Signature Risks

```
----> : Issued by: VeriSign Class 3 Public Primary Certification Authority - G5
----> : Expires: Wed Jul 16 19:59:59 2036
----> : SHA1 hash: 4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5
----> : Issued to: VeriSign Class 3 Code Signing 2010 CA
----> : Issued by: VeriSign Class 3 Public Primary Certification Authority - G5
----> : Expires: Fri Feb 07 19:59:59 2020
----->WARNING: An expired Cert is in the signature chain
Press Enter to acknowledge this warning and continue...
----> : SHA1 hash: 495847A93187CFB8C71F840CB7B41497AD95C64F
----> : Issued to: TeamViewer
----> : Issued by: VeriSign Class 3 Code Signing 2010 CA
----> : Expires: Thu Aug 07 19:59:59 2014
----> : SHA1 hash: 34DB009ABDE83388E437A4CDF44EE43DF3DB1505
----> :The signature is timestamped: Thu Nov 03 16:38:35 2011
----->WARNING: This signature is more than one year in the past
Press Enter to acknowledge this warning and continue...
```

NOTE: Verisign is NOT a NAESB Accredited Certificate Authority

# Vulnerabilities and Exploits

- **ICS Advisory (ICSA-20-133-02)**
- **OSIsoft PI System**
- Original release date: May 12, 2020

## 1. EXECUTIVE SUMMARY

- **CVSS v3 7.8**
- **ATTENTION:** Exploitable remotely/low skill level to exploit
- **Vendor:** OSIsoft
- **Equipment:** PI System
- **Vulnerabilities:** Uncontrolled Search Path Element, Improper Verification of Cryptographic Signature, Incorrect Default Permissions, Uncaught Exception, Null Pointer Dereference, Improper Input Validation, Cross-site Scripting, Insertion of Sensitive Information into Log File

- Exploits; [Top Ten List](#)

## Top 10 Most Exploited Vulnerabilities 2016–2019

U.S. Government reporting has identified the top 10 most exploited vulnerabilities by state, nonstate, and unattributed cyber actors from 2016 to 2019 as follows: CVE-2017-11882, CVE-2017-0199, CVE-2017-5638, CVE-2012-0158, CVE-2019-0604, CVE-2017-0143, CVE-2018-4878, CVE-2017-8759, CVE-2015-1641, and CVE-2018-7600.



# Provenance Risks

- Man in the middle attacks

```
Performing Man in the Middle Trace(this takes a few moments...): ut.ac.ir  
----> ('<DNSBLResult: 80.66.177.54 [BLACKLISTED] (1/52)>', 'UT-AS, IR')  
---->WARNING: Above location is BLACKLISTED  
---->WARNING: Above location is outside of the United States
```

- Watering Holes; e.g. Wordpress
- Spoofed software download locations

Infamous Israeli surveillance firm NSO Group created a web domain that looked as if it belonged to Facebook's security team to entice targets to click on links that would install the company's powerful cell phone hacking technology, according to data analyzed by Motherboard.

It is not uncommon for hackers working for governments to impersonate Facebook, perhaps with a phishing page that displays a Facebook login

# Questions?

Dick Brooks

[dick@reliableenergyanalytics.com](mailto:dick@reliableenergyanalytics.com)

# Common Misconceptions

- A verified digitally signed software object is always trustworthy; NOT TRUE
  - Digitally signed software provides a “veil” of trust that may not be justified
  - [COMODO Fraudulent Certificates](#)  
**Microsoft is aware of nine fraudulent digital certificates issued by Comodo, a certification authority present in the Trusted Root Certification Authorities Store, on all supported releases of Microsoft Windows**
  - [ASUS](#) March 29, 2019  
As *Motherboard* [reported](#), researchers at Kaspersky discovered that malicious hackers had **successfully planted malware posing as an official ASUS security update** onto ASUS’s servers **and signed it with two of the company’s legitimate digital certificates.**
  - [Sophos Threat Report 2020](#)  
Attackers may attempt to minimize detection by **digitally code-signing their ransomware with an Authenticode certificate.**

# Software Vendors Always Patch Known Vulnerabilities Immediately

- NOT TRUE

## **Microsoft fixes vulnerability affecting all Windows versions since 1996**

Another vulnerability in the same Windows component was abused by Stuxnet a decade ago



Amer Owaida 15 May 2020 - 03:30PM

# All Vendors Follow Secure Coding Standards; NOT TRUE

- <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04232020.pdf>

NIST CYBERSECURITY WHITE PAPER  
APRIL 23, 2020

MITIGATING THE RISK OF SOFTWARE  
VULNERABILITIES BY ADOPTING AN SSDF

## Abstract

Few software development life cycle (SDLC) models explicitly address software security in detail, so secure software development practices usually need to be added to each SDLC model to ensure the software being developed is well secured. This white paper recommends a core set of high-level secure software development practices called a secure software development framework (SSDF) to be integrated within each SDLC implementation. The paper facilitates communications about secure software development practices among business owners, software developers, project managers and leads, and cybersecurity professionals within an organization. Following these practices should help software producers reduce the number of vulnerabilities in released software, mitigate the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences. Also, because the framework provides a common vocabulary for secure software development, software consumers can use it to foster communications with suppliers in acquisition processes and other management activities.

# You must protect yourself

- You cannot be assured that a vendor is aware of the risks that are inherent in their software or the supply chain used by your Company to acquire their software
- If a breach occurs in your Company, then you will be the one accountable for the damage and costs to recover (not the SW vendor/supplier), along with any non-compliance fines
- You cannot “outsource” all of the cost of a breach, i.e. recovery efforts and the harm to reputation from a successful cyber attack on your Company,
- But you can try to detect risks
- Would you take a free drink from a stranger in a bar? Software should be viewed in the same way!
- Never trust software, always verify and report!<sup>TM</sup>

# Ongoing Due Diligence

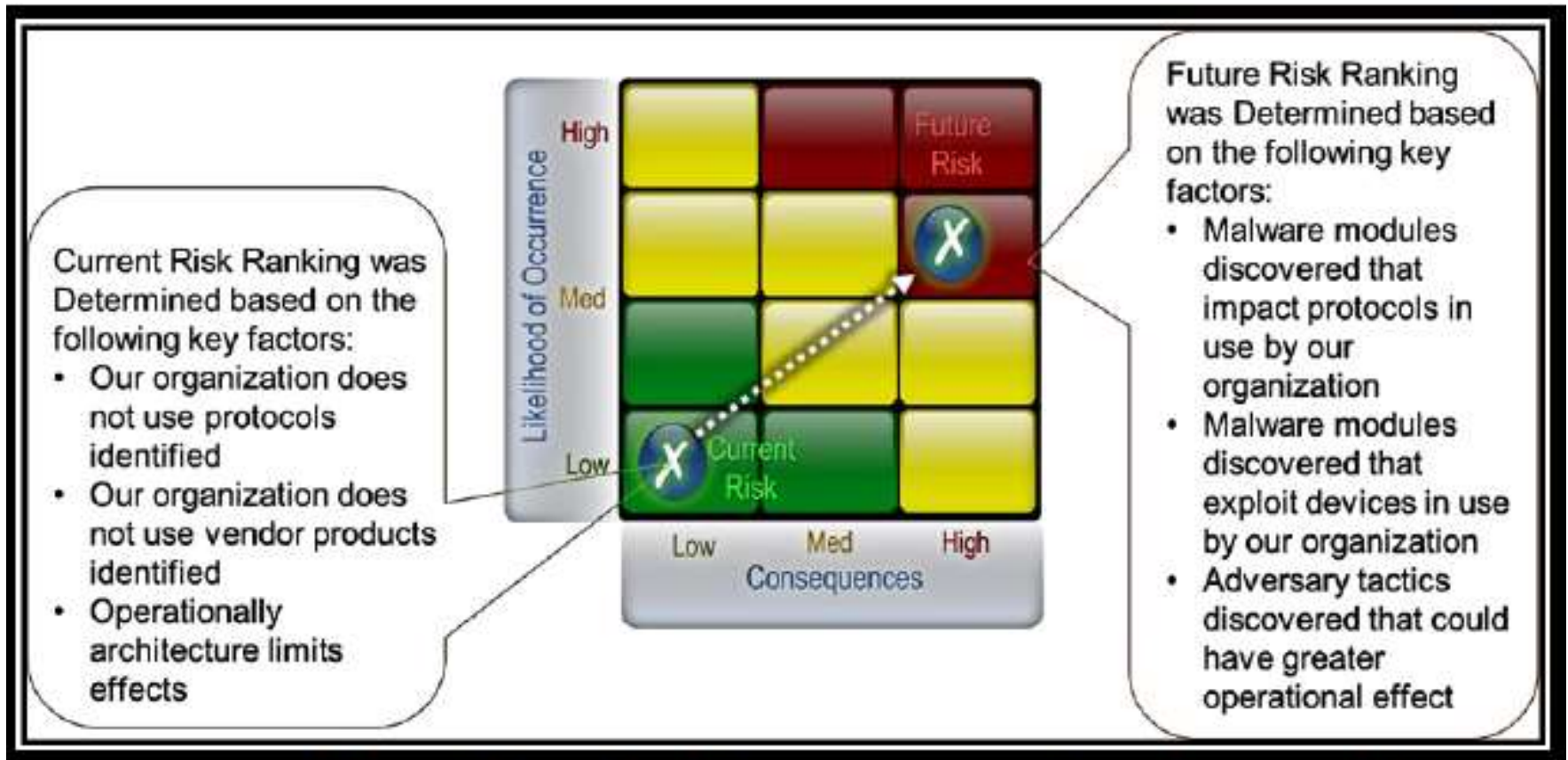
- Implement software integrity and authenticity controls following the technical guidelines contained in NERC CIP-010-3 augmented by the enhanced best practices provided in the NIST Cybersecurity Framework
- Follow FERC's suggestions:
  - *"Standards do not necessarily require entities to employ best practices"*
  - *"augmenting the current CIP Reliability Standards under FPA section 215 with an incentive-based approach under FPA section 219 that encourages utilities to undertake cybersecurity investments on a voluntary basis. This approach would incentivize a utility to adopt best practices to protect its own transmission system as well as improve the security of the BES"*
- The NIST CSF contains a comprehensive set of guidelines of cybersecurity best practices that are intended to protect the Bulk Electric System, above and beyond NERC CIP-010-3 standards
- Cybersecurity is a cat and mouse game that requires constant vigilance
- Security risks don't stand still and neither should your software cybersecurity risk controls, in order to remain effective
- FERC Order 850, Mandatory Supply Chain Standards, are scheduled to go into effect on 10/1/2020 (18 CFR 40); it can take several months to setup effective risk management controls to satisfy NERC compliance requirements and apply effective best practices following the NIST CSF

# Summary

- Software Supply Chain breaches are costly to recover from and can adversely effect Company finances and reputation (and your own career)
- Apply prudent risk management controls following NIST CSF best practices and NERC CIP-010-3 to detect risks and threats to the Bulk Electric System, and meet NERC compliance requirements
- No risk management control is guaranteed to protect you from harm, but some are useful
- Software supply chain risk assessments should include both vendor centric (CIP-013) and software centric risk (CIP-010-3) analysis
- You cannot rely on vendors to protect you from harm; you alone are accountable for your own security!



# When Reality Sets In



**Figure 15: Current Risk Ranking and Assessment of Potential Risk**

# Questions?

Dick Brooks

[dick@reliableenergyanalytics.com](mailto:dick@reliableenergyanalytics.com)

# Acknowledgements

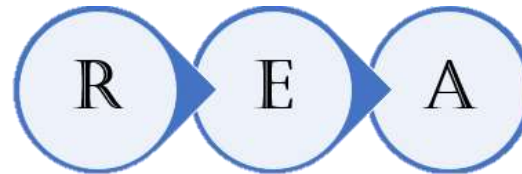
- Many thanks to [Tom Alrich](#) for providing valuable insights on NERC CIP-013-1.
- I highly recommend following his NERC CIP blog postings here: <http://tomalrichblog.blogspot.com/>

# Reliable Energy Analytics LLC

- Established December 2018
- Developer of patent pending Software Assurance Guardian™ (SAG) Methodologies and Technologies
- Provider of Software Risk Management controls to meet NERC CIP-010-3 and FERC Order 850 regulations on 10/1/2020; [SAG Point Man software \(SAG-PM™\)](#)
- Extensive Energy industry experience, since 1990, delivering secure, mission critical software solutions
- 14 years with ISO New England responsible for enterprise architecture, Advanced Data Analytic solutions, NAESB PKI standards and implementation
- Active member of the North American Energy Standards Board (NAESB), serving as Vice Chairman on the Wholesale Electric Quadrant (WEQ) Executive Committee
- [Never trust software, always verify and report!™](#)

# Contact Information

Dick Brooks



Reliable Energy Analytics LLC

[dick@reliableenergyanalytics.com](mailto:dick@reliableenergyanalytics.com)

Energy Central:

<https://energycentral.com/member/profile/225424/about>

Tel: 978-696-1788

[Never trust software, always verify and report!™](#)

Thank you and thanks to our  
sponsors!

