PATCHING LESSONS LEARNED:
An Interesting Perspective
WHO WE ARE

MISSION
We ensure the success of our customers by developing innovative technology solutions that optimize and protect critical infrastructure.

HISTORY
- Company was started in 1981. Happy 36th birthday to us!
- 25+ years of experience in the design, manufacture, and lifecycle management of industrial HMIs and SCADA devices
- 11+ years of experience working with cyber security in the energy industry
- ISO 9001:2008 certified
- In 2013, we were awarded a $4.3M cooperative agreement by the Department of Energy in the Cybersecurity for Energy Delivery Systems (CEDS) Program
- In 2014, we merged the computing and cyber security businesses under the name of FoxGuard Solutions
- Total employees = ~110
FoxGuard serves as a solution provider for mission-critical applications in Critical Infrastructure and Key Resource (CIKR) sectors.

**Our Solutions Fall Into Three Primary Categories:**

1. Cyber Security
2. Compliance
3. Industrial Computing Hardware
PATCH & UPDATE MANAGEMENT PROGRAM

Patch & Update Data Aggregator/Web Portal

- Provides users a with single location to find information about patches and updates applicable to energy delivery industrial control system devices
- The portal serves as a repository for Hash Authentication information, patch discovery evidence and device End of Support (EOS) documentation

Patch & Update Authentication

- Our aggregated Hash Files from vendors provide users a central location to help verify the integrity of downloaded patches and updates prior to deployment
- The Hash Authentication Tool allows customers receiving aggregated patch data via customized reports to authenticate that reports have not been compromised

Validation Techniques

- Provides users with proven methodologies to validate patches and updates before deployment
- Users may self-perform, set up their own validation lab, contract validation services or take a combined approach

Query Engine

- The Query Engine will support multiple device types and across various energy delivery ICS vendors
- Enables users to query IT and OT equipment to determine relevant baseline information such as Make, Model, Firmware Version and Serial Number – this information is critical for accurate patch discovery
- The Query Engine will offer an easy to use user interface supporting a Patch Gap Analysis Dashboard simplifying the process of determining your current patch status and gaps
FoxGuard Solutions builds customized programs that function as an extension of the customer’s organization, enabling them to provide easy to use, easy to manage cyber security to their controls while ensuring their reliability.

- FoxGuard is currently managing &
  - 114 Companies
  - 181 Sites
  - 36 States
  - 30 Countries
COMPANIES USING FOXGUARD -

TOSHIBA

GREAT RIVER ENERGY

Progress Energy

INTERNATIONAL PAPER

MTU Maintenance

nrg

FPL

G E Energy

SOUTHERN CALIFORNIA EDISON

Sentinel Energy Project

New York Power Authority

SSE

TempleInland

CONSOLED ENERGY COMPANY

conEdison

IBERDROLA

SCE & G

TECTEN

NIPSCO

AES

ExxonMobil

Colorado Springs Utilities

GDF Suez

KUA

FirstEnergy

IPL

TVA

Clark Public Utilities

SCE & G

Platte River Power Authority

Dynegy

Kansas City Board of Public Utilities

bp

U AMPS

ALLIANT ENERGY

TransCanada

Raytheon

NAES

Enel

Entergy
PATCHING. -
How Hard Can It Be? -

Harder than you think. Trust us. &
WHAT IS A PATCH?

- Feature Enhancements And / Or Security Patches

- Focus Is On The Security Patches, As These Address Vulnerabilities To Their Company (Not To Mention Compliance Requirements)
WHAT NEEDS PATCHES & UPDATES -

OPERATING SYSTEMS

3RD PARTY APPLICATIONS

SUPPORTED ASSETS

NETWORK DEVICES

FIELD DEVICES

Cyber Security | Compliance | Industrial Computing
Why is Patch Management important?

- Energy Utilities are high-risk targets

- Patches are crucial
  - 189 known vulnerabilities in ICS in 2015*
  - 26 had exploits available*
  - 170 had patches available*

- NERC CIP says so
  - CIP-007-6 R2.1, R2.2, R2.3, R2.4
  - Large fines for failure to comply

*Kaspersky Labs Industrial Control Systems Vulnerabilities Statistics
Current State

- Existing solutions:
  - Are fragmented with limited coverage
  - Do not provide standardized actionable output
  - Have widely varying capability sets
- Changing/increasing compliance scope
### Compliance -

<table>
<thead>
<tr>
<th>Part</th>
<th>Applicable Systems</th>
<th>Requirements</th>
<th>Measures</th>
</tr>
</thead>
</table>
| 2.1  | High Impact BES Cyber Systems and their associated:  
1. EACMS;  
2. PACS; and  
3. PCA  
Medium Impact BES Cyber Systems and their associated:  
1. EACMS;  
2. PACS; and  
3. PCA | A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists. | An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis. |
## Compliance

<table>
<thead>
<tr>
<th>Part</th>
<th>Applicable Systems</th>
<th>Requirements</th>
<th>Measures</th>
</tr>
</thead>
</table>
| 2.2  | High Impact BES Cyber Systems and their associated:  
1. EACMS;  
2. PACS; and  
3. PCA | At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1. | An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days. |
<table>
<thead>
<tr>
<th>Part</th>
<th>Applicable Systems</th>
<th>Requirements</th>
<th>Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3</td>
<td>High Impact BES Cyber Systems and their associated:</td>
<td>For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions:</td>
<td>Examples of evidence may include, but are not limited to:</td>
</tr>
<tr>
<td></td>
<td>1. EACMS;</td>
<td>• Apply the applicable patches; or</td>
<td>• Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or</td>
</tr>
<tr>
<td></td>
<td>2. PACS; and</td>
<td>• Create a dated mitigation plan; or</td>
<td>• A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.</td>
</tr>
<tr>
<td></td>
<td>3. PCA</td>
<td>• Revise an existing mitigation plan.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Medium Impact BES Cyber Systems and their associated:</td>
<td>Mitigation plans shall include the Responsible Entity’s planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.</td>
<td></td>
</tr>
</tbody>
</table>
### Compliance

<table>
<thead>
<tr>
<th>Part</th>
<th>Applicable Systems</th>
<th>Requirements</th>
<th>Measures</th>
</tr>
</thead>
</table>
| 2.4  | High Impact BES Cyber Systems and their associated:  
   1. EACMS;  
   2. PACS; and  
   3. PCA |
|      | Medium Impact BES Cyber Systems and their associated:  
   1. EACMS;  
   2. PACS; and  
   3. PCA |
|      | For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate. |
|      | An example of evidence may include, but is not limited to, records of implementation of mitigations. |
Security

- Installing patches mitigates risks from vulnerabilities
- Increased reliability of services may occur as a result of patching
- “Air-gapped” is not enough
- Compliance only mandates “security patches” be installed, but non-security patches may offer functionality that leads to security features.
- Near real-time application of patches and/or mitigation
- Zero Day is a real thing. (Forever Day is a real thing too. Security holes that remain unpatched. – Unfixed vulnerabilities – usually with legacy applications.)
Understanding IT vs. OT is Critical

- OT devices are not and SHOULD NOT be treated as IT devices – Need expertise to understand and manage the differences &

- Not all vendors report current patch status every month so you must contact them directly. (Keep track of these vendors.)

- Regular patch notification for some OT vendors is a new & concept &
Public AND Private Patches – Which are Which?

- Approximately half of all EDS have “Private” patches
  - Not readily available on the Internet
  - Must securely track credentials
  - Understand requirements for obtaining this information
    - Private Portal, Current Support Contract, Call, Newsletter, etc.
Patch Analysis Accuracy is Difficult -

- Documenting the process (where to go, how to mine, etc.) is an on-going effort
- The mining procedure changes with each vendor
- Vendors are known to change their process
- Some products can be intricate and time consuming to find details
  - Ex. Cisco –
    - Security bugs are listed individually
    - Security ratings are buried within Release Notes
    - Multiple CVE’s may be listed
Asset Analysis is Complicated

- On-Going effort – Keeping it “current” is hard
- Sub-components
  - Numerous distinct software packages on HMI/SCADA devices
- Vendor Ownership of Asset (may have many vendors that distribute a & product)
- Support Provider (may be different from initial Vendor)
- Obtaining sufficient information in order to patch properly
- IT Contractors may help but are not bullet proof
- Aggregate lists may not be sufficient – Each asset may be different, even if it seems the same (i.e., serial number, patch status)
Check Point R7X and R8X Release Map

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend:
- EOS = End of Support
- Integration to other release

IMPORTANT:
Check Point recommends that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Last Update: Mar 2016
Security vs. Non-Security Determination takes Knowledge -

- Not all vendors provide security rating
- Need the resources and expertise to determine, if a vendor doesn’t provide
- CVE Information and CVSS Scores are helpful, but are not always provided &
- Vulnerabilities are not always updated by the vendor
A Patch is not a Patch is not a Patch

- Several types of patches:
  - Cumulative – One installation includes previous installation (Microsoft’s new model)
  - Independent – Each patch can be installed independent from others (Current patch status may be difficult to track)
  - Primary/Dependent – Must have a previous installation before installing the latest (Keep track of what installed)

- Patches can be changed/rereleased/retracted

- Back Dating patches is possible (Vendor releases today but is dated three months ago.)
October 24, 2016

Three Patches

December 2, 2016
Download Software

October 24, 2016

Four Patches

December 28, 2016
Maintaining Evidence is Hard

- Types of Documentation
  - Patch Documentation
    - Proof you checked
    - Record status at the time you checked
  - EOS Documentation
    - Not every product lives forever
    - Audit-ready documentation must be created
    - Indicate change in status over the course of product lifetime

- Time Consuming
- What is appropriate – “Audit-worthy”
- Maintaining – Keeping up to date, as well as storage of documents
- Audit trail
Your Calendar with Many Sources is Timely to Manage
Time & Resource Intensive

- Patch Discovery takes MANY hours every month
  - Contact vendors
  - Who to call?
  - Email?
  - Website?
  - Newsletter?
  - Automatically provided?
  - Maintain timeline for each vendor – 35 days?
  - Documentation, documentation, documentation
Validation is Intricate

- **Scope**
  - What to test, What level of detail (registry change applied to which patch, file versions, specific changes in a shared XML file, etc.

- **Resources**
  - People - Need the right people with the right training to understand this process
  - Equipment – Needs to have access to a representative system (production/lab, physical/virtual

- Test Equipment – Need equipment different from what you need in & production in order to test the system &
# Validation Standard

<table>
<thead>
<tr>
<th>Part</th>
<th>Applicable Systems</th>
<th>Requirements</th>
<th>Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.5</td>
<td>High Impact BES Cyber Systems</td>
<td>Where technically feasible, for each change that deviates from the existing baseline configuration:</td>
<td>An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.</td>
<td></td>
</tr>
</tbody>
</table>
The Risks:

- Safety:
  - Improperly Patched - “Brick” a device or Create a false sense of security
  - Temporal Vulnerability with a missed patch – The longer you go without patching, the greater your vulnerability/risk

- Reliability:
  - Impact on The Grid? Reliability is critical.

- Efficiency:
  - Stay focused on the job at hand and leave patching to the experts
  - Compliance Risks – Fines for non-compliance
The Lessons:

- Understanding IT vs. OT is Critical
- Public AND Private Patches – Which are Which?
- Patch Analysis Accuracy is Difficult
- Asset Analysis is Complicated
- Security vs. Non-Security Determination takes Knowledge
- A Patch is not a Patch is not a Patch
- Maintaining Evidence is Hard
- Your Calendar with Many Sources is Timely to Manage
- Time & Resource Intensive
- Validation is Intricate

IS YOUR PROGRAM ORGANIZED? ARE YOU READY?
THE BENEFITS OF A HEALTHY PATCHING PROGRAM

End User Benefits
- Centralizes patch and update information
- Supports programmatic equipment querying using automation and a common toolset
- Simplifies association between software and available patches / updates
- Lower cost with scalability of the program
- More accurate information
- Recurring delivery of information

Cyber Security Advancements
- Promotes end user awareness around patching, presence of vulnerabilities and change management processes &
- Provides common security classification in absence of vendor classification
- Considers named sub-components and libraries to provide more comprehensive security assessment &
- Reduces likelihood of incorrect patch application
- Standardizes presentation of patch information to end user
FoxGuard Solutions Offers:

- Patch Management
- Security Services
- Integrated Security Solutions
- Industrial Computers
- And Many Other Custom Solutions

For more information please contact:

Michele Wright  
Product Manager  
(540) 382 – 4234 x244  
mwright@foxguardsolutions.com

Lindsey Hale  
Program Manager  
(540) 382 – 4234 x108  
lhale@foxguardsolutions.com
WANT TO LEARN MORE ABOUT PATCH MANAGEMENT

We can do that too! FoxGuard hosts a webinar series to discuss ways to develop and implement a robust patch management program. Visit our website to reserve a spot today.

http://foxguardsolutions.com/patch-management-webinar

If you want to discuss something specific, we will do that too. Just reach out, tell us what your challenges are, and we will have one of our security experts contact you.

http://www.foxguardsolutions.com/contact

- www.foxguardsolutions.com
- requestinfo@foxguardsolutions.com
- 877.446.4732
- company/717871
- @FoxGuardInc