A Holistic Approach to Cyber Security

Security Software Development Life Cycle

- Security Requirements
  - Design Criteria
    - Defense in Depth
    - Least privileges, and more
  - Security Architecture
- Secure Design
  - Security Features
    - Centralized user account management
    - Data security, log management
- Secure Coding
  - Cutting Edge Technologies
    - WS Security, HTTPS, TLS, SSO, 2-factor authentication, & more
- Security Testing
  - Compliance!

Tools

National Cyber Storm
Defense in Depth

Specify the network security zones

Must work with firewalls and IDS/IPS

Support anti-virus software

Support content inspection

Least privileges

Adopt standards

Integrate with 3rd party security solutions
Security Features

• Authentication and Authorization
  − Centralized user account management
  − Utilize standard user management services
  − Support 2-factor authentication
  − Support Single-Sign-On

• Data Security
  − Secure data in storage, in transit, and in memory
  − Use standard security protocols: SSL/TLS, HTTPS, WS-Security, etc.

• Log Management
  − Support log standard: syslog
  − Integrate with enterprise logging management solution
Secure Design Specifications and Standards
Secure Design

- Microsoft Threat Analysis and Modeling Tool
- Developers training by Microsoft
Secure Coding

- Provide secure coding training to developers
- Scan source code using Fortify SCA
- Require source code peer review
Security Software Development Lifecycle

Security Testing

• Alstom Grid Internal Security Testing

• Independent Security Vulnerability Testing
  – DOE NSTB
  – DHS CSSP
  – 3rd party security company
Documented Security Best Practices

Deployment - System Hardening

• **e-terra** Security Guides
  - **e-terra** Security Overview
  - **e-terra** Network Security Guide
  - **e-terra** System Security Guide – Windows
  - **e-terra** System Security Guide – Linux
  - **e-terra** Secure Shell (SSH) User’s Guide
  - **e-terra** Secure Connection User’s Guide
  - **e-terra**trust User’s Guide

  ![Diagram showing system hardening components](image-url)
Welcome to The Support Portal

Operating System Patch Testing Results

This section describes procedures and results for Alstom Grid testing of operating system vendor security patch compatibility with designated Alstom Grid applications, versions and OS platforms.

You will find all information in this page. To select the Security Patch of your choice, please proceed as following:

- **Build below your selection list** using one or several criteria then click on **Search**
  (note: it takes few seconds)
- **Access to more details** on a specific Patch Test Result by double-clicking on the line.
  (note: your browser must allow pop-up windows)

OS Patch Testing Results

<table>
<thead>
<tr>
<th>Mfg</th>
<th>Year</th>
<th>Product</th>
<th>OS</th>
<th>Rating</th>
<th>Patch ID</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS</td>
<td>2011</td>
<td>Windows Fax</td>
<td>Windows 2008</td>
<td>Normal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS</td>
<td>2011</td>
<td>Windows Kernel-Mode Drivers</td>
<td>Windows 2008</td>
<td>Normal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS</td>
<td>2011</td>
<td>Windows Media</td>
<td>Windows 2008</td>
<td>Normal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS</td>
<td>2011</td>
<td>Windows Kernel</td>
<td>Windows 2008</td>
<td>Normal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS</td>
<td>2011</td>
<td>Windows Kernel-Mode Drivers</td>
<td>Windows 2008</td>
<td>Normal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS</td>
<td>2011</td>
<td>Windows 2008 Impor</td>
<td>MS11-012</td>
<td>Normal</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Click Here to learn more about above links
Ensuring System Security

Automatic System Auditing

• The Bandolier Audit Files
  – The audit files document optimal security configurations for Alstom SCADA control systems
  – Cost effective ongoing monitoring by asset owners
  – Auditable report for compliance
    • NERC CIP, NIST, FISMA, ISA-99 and etc.

- terra platform 2.5 (habitat 5.7)
  - Windows Server 2003
  - Windows XP
  - Red Hat 5.3
- terra platform 2.6 (habitat 5.8)
  - Windows Server 2008 R2
  - Windows 7
  - Red Hat Linux 5.5
Vulnerability Response and Disclosure

Alstom Grid Security Bulletin URL

Welcome to the SUPPORT PORTAL

Welcome Sharon Xia

SECURITY CORNER

User Information
- OS Patch Testing
- Monthly Test Results
- Test Results Key
- Testing Overview / FAQ
- Product Security Bulletins
- Security Technical Flashes

Security Services
- Security Assessment
- Patch Management
- System Hardening

Other Resources
- Security Focus Group
- INL Vulnerability Testing Program
- Standards and Guidelines
- AREVA Security Recommendations

Product Security Bulletins
The following table lists Product Security Bulletins issued for AREVA T&D products. These bulletins provide detailed information on security-related issues which have been identified, and suggest methods to resolve these problems on affected product versions / platforms.

Product Security Bulletins are listed in reverse chronological order. Click on the bulletin ID hyperlink to view the full text of the corresponding security bulletin.

<table>
<thead>
<tr>
<th>Bulletin</th>
<th>Title</th>
<th>Impact</th>
<th>Severity</th>
<th>Vulnerability ID (SPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATD-10-001</td>
<td>Multiple Vulnerabilities in e-terracommo ICPPLINK</td>
<td>Remote Denial of Service or Remote Code Execution</td>
<td>Critical</td>
<td>PD35952 PD35953 PD35964 PD35966</td>
</tr>
</tbody>
</table>