RT LOGIC
technology that connects

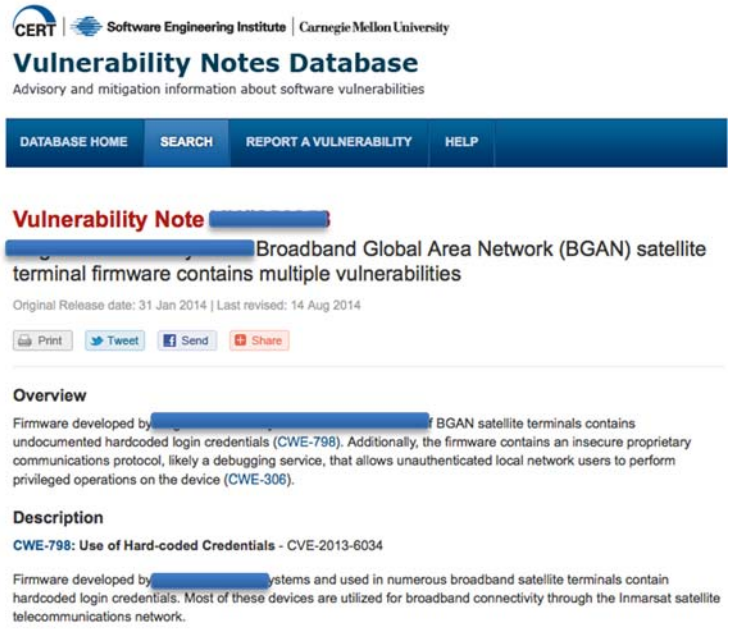
Real-time Cyber Situational Awareness for Satellite Ground Networks

March 2015

Presenter: Ted Vera

Recent Attacks

- **NOAA allegedly hacked by China**
  - Washington Post (11/14)
- **15yr Old Hacks NASA Computers that support ISS**
  - ABC (09/14)
- **Hacking Satellites – Look up to the Sky**
  - Infosec Institute (09/14)
- **Satellite Hacking for Fun & Profit**
  - Blackhat (02/09)
- **NASA Terra EOS & LandSat-7 allegedly hacked by China (2007 & 2008)**
  - US-China Economic & Security Review Commission (11/11)


CERT | Software Engineering Institute | Carnegie Mellon University

Vulnerability Notes Database

Advisory and mitigation information about software vulnerabilities

DATABASE HOME | SEARCH | REPORT A VULNERABILITY | HELP

Vulnerability Note [redacted]

[redacted] Broadband Global Area Network (BGAN) satellite terminal firmware contains multiple vulnerabilities

Original Release date: 31 Jan 2014 | Last revised: 14 Aug 2014

Print | Tweet | Send | Share

Overview

Firmware developed by [redacted] BGAN satellite terminals contains undocumented hardcoded login credentials (CWE-798). Additionally, the firmware contains an insecure proprietary communications protocol, likely a debugging service, that allows unauthenticated local network users to perform privileged operations on the device (CWE-306).

Description

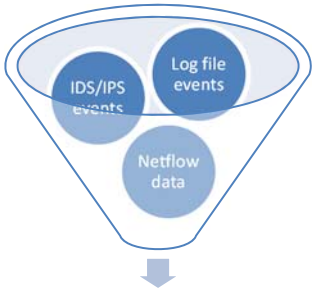
CWE-798: Use of Hard-coded Credentials - CVE-2013-6034

Firmware developed by [redacted] ystems and used in numerous broadband satellite terminals contain hardcoded login credentials. Most of these devices are utilized for broadband connectivity through the Inmarsat satellite telecommunications network.

Satellite ground networks are exposed to increasing number of targeted cyber threats

Cyber Situational Awareness with SIEM

- **What is a Security Information & Event Manager (SIEM)**
  - Sensors, Loggers, Analysis Engine, GUI
- **Aggregates data from multiple sources**
  - Log files, Network Traffic, AV, IPS, HIDS
- **Analysis Engine**
  - Correlates events into actionable alerts
- **Visualization / GUI**
  - Prioritized Alarms, Alerts, and Notifications
  - Dashboard, Reports, Trends
- **Limitations**
  - Do not actively prevent attacks or enforce policies

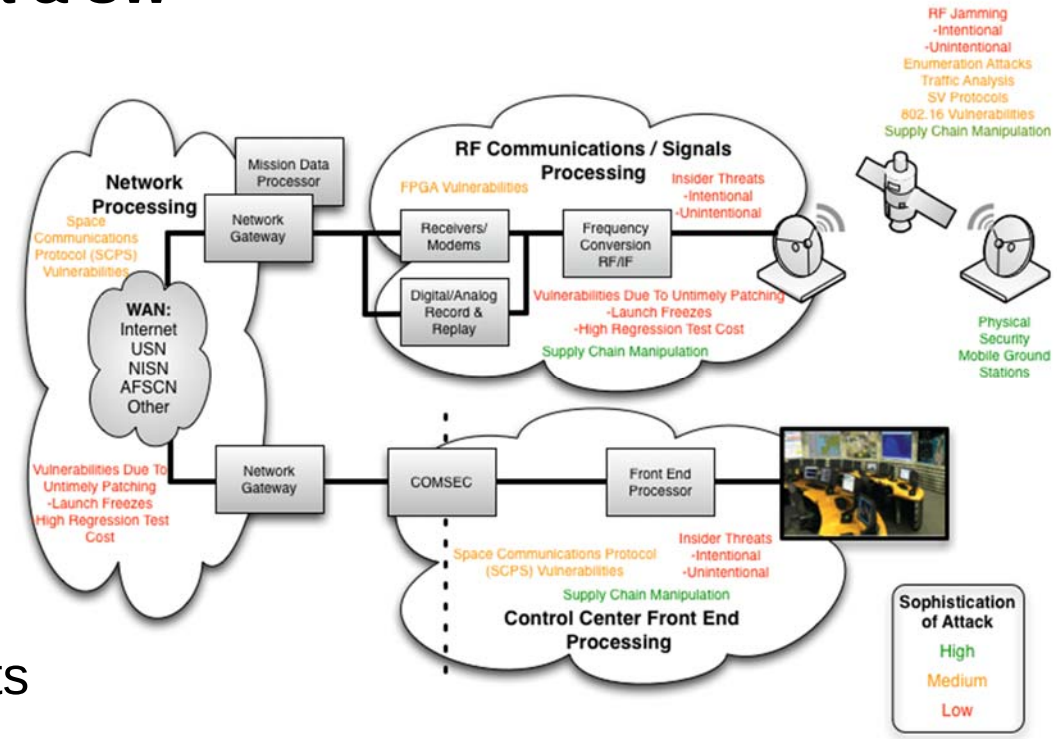


Actionable Information & Automated Responses

Use of SIEMs in private sector has become industry accepted best practice

Satellite Ground Network Threatscape

- **“Traditional” IP threats plus…**
- **Mission Unique Equipment & SW**
- **Serial COMMS**
  - Insecure protocols
- **Specialized Protocols**
  - ie: SCPS, GEMS, etc
- **Deprecated protocols**
  - ie: Telnet, FTP, SNMPv1
- **Untimely patching due to**
  - Launch Freezes
  - High regression test costs
- **RF Attacks**



Satellite ground networks have mission unique attack surfaces

RT LOGIC
technology that connects

Mission Unique Equipment (MUE)

- **IOActive published a vulnerability assessment of common SATCOM MUE (4/14)**
- **Numerous significant findings**
  - Backdoors
  - Hardcoded credentials
  - Insecure protocols
  - Undocumented protocols
  - Weak password reset
  - Vulnerable to spoofing

"Santamarta showed how he was able to gain access to satellite data units … through so-called backdoors and hard-coded credentials in firmware."

Vulnerability Class	Service	Severity
Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN	Critical
Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN BGAN M2M	Critical
Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	Thuraya Broadband	Critical
Weak Password Reset Insecure Protocols	BGAN	Critical
Weak Password Reset Insecure Protocols Hardcoded Credentials	VSAT	Critical
Backdoors Weak Password Reset Insecure Protocols Hardcoded credentials	SwiftBroadband Classic Aero	Critical
Weak Password Reset Insecure Protocols	FB	Critical
Insecure Protocols Hardcoded Credentials	Inmarsat-C	Critical
Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	FB	Critical
Hardcoded Credentials Undocumented Protocols	Iridium	Critical

Mitigate MUE risks through continuous monitoring using SIEM

SIEM Challenges & Opportunities

- **SIEM Tailoring & Tuning**
- **Lack of plugins for MUE**
  - Parsers normalize log data - put security context around events
  - Correlate IP & RF events logged by MUE along a timeline
- **Lack of plugins/rules for specialized/deprecated protocols**
  - Plugins & rules to monitor specialized/deprecated protocols
- **Post-processing events from deployable ground systems**
  - Ability to ingest logs and generate alerts/alarms/reports
- **Operating in Cross-Domain Environments**
  - Cost of Master SIEMs vs Sensors
  - Benefit of having real-time Enterprise situational awareness

Tailoring and Tuning a SIEM is required for any environment

RT LOGIC
technology that connects

SIEM Benefits

- **Alerts & alarms provide decision makers with near real-time Cyber security situational awareness**
- **Makes analysts more effective by automating monitoring and prioritizing alarms**
- **Streamlines log audits and compliance reporting**
  - Commercial & DoD standards
- **Mitigates MUE risks by monitoring known vulnerabilities**
- **Mitigates deprecated protocol risk by monitoring usage**
- **Improves response time and efficiency of incident response activities with searchable, centralized logs**
- **Helps organization satisfy continuous monitoring requirements**

Improve the security posture of your satellite ground network with a SIEM

Questions & Contact Info

Questions?

Contact Information:

Ted Vera

Tel: 719-598-2801

Email: tvera@rtlogic.com