GVF Cyber Security Task Force

Update on Activities and Security Implications for HTS

Martin Jarrold, GVF Chief of International Programme Development

Rakesh Bharania

Chair, GVF Security Task Force
Network Consulting Engineer, Cisco Tactical Operations

2016

Satellite. Solutions. The World.

Media reports of VSAT security

GVF Response

GVF Product Security Baseline (PSB)

Satellite Service Provider Security Document (SSPSec)

Conclusion…

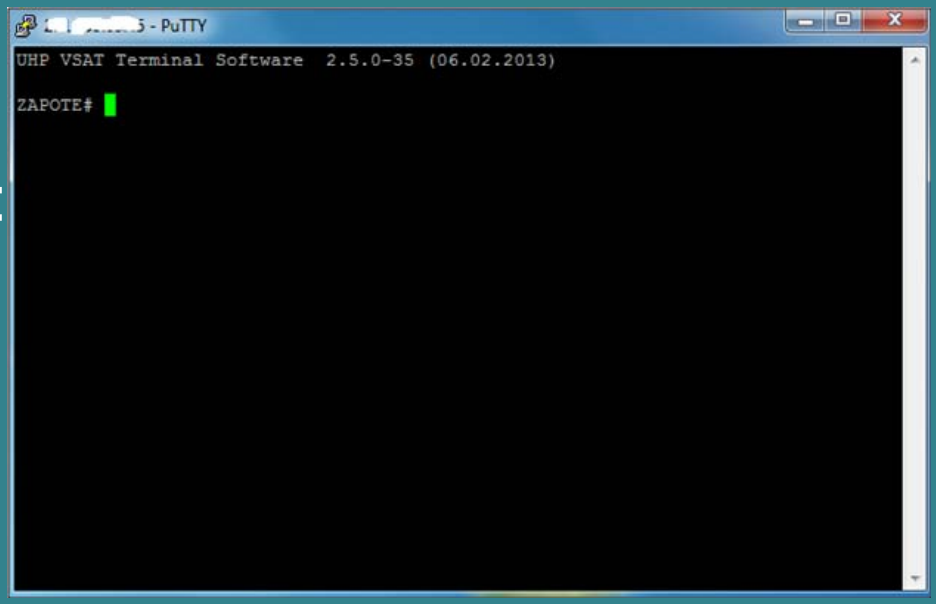
Timeline of recent media reports…

GVF Satellite. Solutions. The World.

Timeline: VSAT Security In the Media

1/9/2014: IntelCrawler report:

Scan of entire IPv4 address space “found approximately 313 open UHP VSAT Terminals, 9045 open HUGHES Terminals, 1142 SatLink VSAT”, “use of default passwords, telnet”



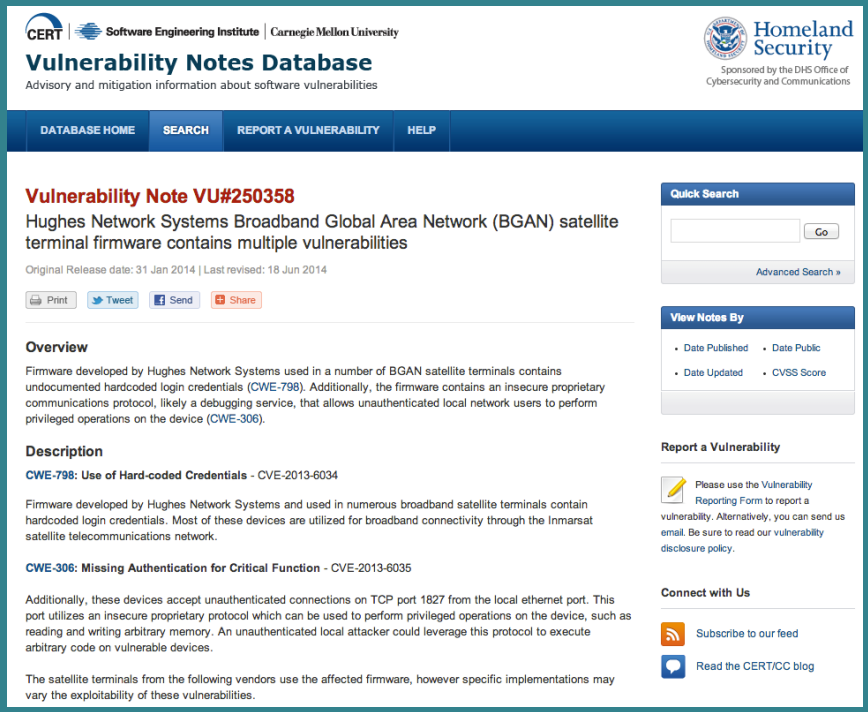
GVF Satellite. Solutions. The World.

Timeline: VSAT Security In the Media

1/31/2014: CERT/CC Publishes Bulletin on BGAN

Vulnerability Note VU 250358:

"Firmware developed by Hughes Network Systems used in a number of BGAN satellite terminals contains undocumented hardcoded login credentials (CWE-798) … contains insecure proprietary protocol on TCP 1827 that can be used to perform privileged operations (CWE-306)



CERT | Software Engineering Institute | Carnegie Mellon University

Vulnerability Notes Database

Advisory and mitigation information about software vulnerabilities

Homeland Security

Sponsored by the DHS Office of Cybersecurity and Communications

DATABASE HOME | SEARCH | REPORT A VULNERABILITY | HELP

Vulnerability Note VU#250358

Hughes Network Systems Broadband Global Area Network (BGAN) satellite terminal firmware contains multiple vulnerabilities

Original Release date: 31 Jan 2014 | Last revised: 18 Jun 2014

Print | Tweet | Send | Share

Overview

Firmware developed by Hughes Network Systems used in a number of 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 Hughes Network Systems 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.

CWE-306: Missing Authentication for Critical Function - CVE-2013-6035

Additionally, these devices accept unauthenticated connections on TCP port 1827 from the local ethernet port. This port utilizes an insecure proprietary protocol which can be used to perform privileged operations on the device, such as reading and writing arbitrary memory. An unauthenticated local attacker could leverage this protocol to execute arbitrary code on vulnerable devices.

The satellite terminals from the following vendors use the affected firmware, however specific implementations may vary the exploitability of these vulnerabilities.

Quick Search | Go | Advanced Search »

View Notes By: Date Published | Date Public | Date Updated | CVSS Score

Report a Vulnerability

Please use the Vulnerability Reporting Form to report a vulnerability. Alternatively, you can send us email. Be sure to read our vulnerability disclosure policy.

Connect with Us

Subscribe to our feed

Read the CERT/CC blog

Timeline: VSAT Security In the Media

20/02/2014: GVF Announces Cybersecurity Task Force

"…global initiative to address escalating cyber-security threats with the establishment of a task force that will identify best practice and provide guidance on how users and industry can optimize the application of VSATs to reinforce network integrity."

GVF Satellite. Solutions. The World.

Timeline: VSAT Security In the Media

17/04/2014: IO Active report

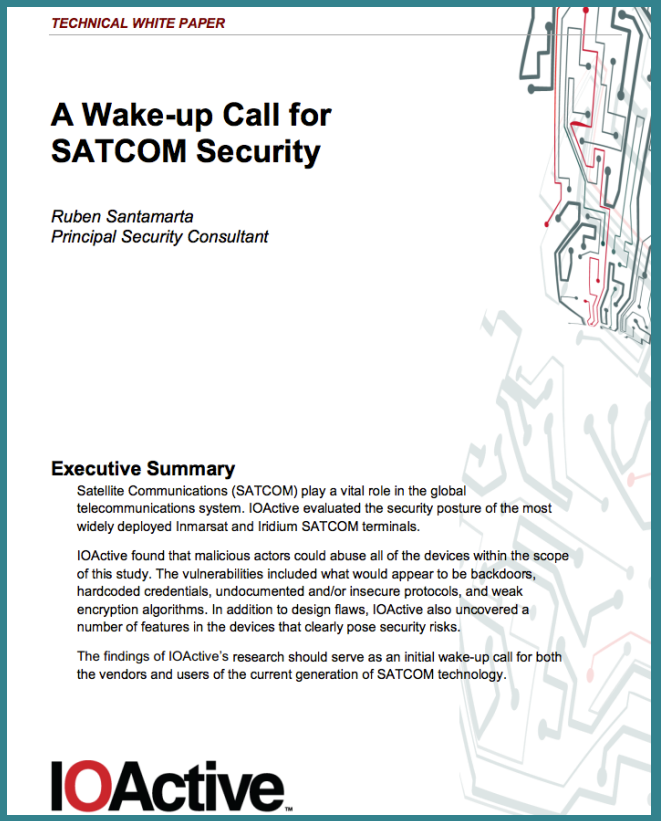
"A Wake up Call for SATCOM Security"

Discussed vulnerabilities in Harris, Hughes, Thuraya, Cobham, JRC, Iridium products

Attacks included: backdoors, hardcoded credentials, insecure and undocumented protocols, weak password reset mechanisms.

Attempted coordinated disclosure with vendors & CERT/CC, but only Iridium responded to inquiries.

HUGE media uptake: industry press, BBC, Wired, Ars Technica, Christian Science Monitor, 60+ articles written



TECHNICAL WHITE PAPER

A Wake-up Call for SATCOM Security

Ruben Santamarta
Principal Security Consultant

Executive Summary

Satellite Communications (SATCOM) play a vital role in the global telecommunications system. IOActive evaluated the security posture of the most widely deployed Inmarsat and Iridium SATCOM terminals.

IOActive found that malicious actors could abuse all of the devices within the scope of this study. The vulnerabilities included what would appear to be backdoors, hardcoded credentials, undocumented and/or insecure protocols, and weak encryption algorithms. In addition to design flaws, IOActive also uncovered a number of features in the devices that clearly pose security risks.

The findings of IOActive's research should serve as an initial wake-up call for both the vendors and users of the current generation of SATCOM technology.

IOActive

Product Security Baseline

The GVF Product Security Baseline

Voluntary specification created by the members of the task force

Representation from vendors, network operators, end-users of VSAT (FSS/MSS)

Details requirements and recommendations for all VSAT hardware and software that supports or transmits on an IPv4 or IPv6 network.

Details requirements and recommendations for all VSAT equipment and software vendors for vulnerability management, disclosure, etc.

GVF Satellite. Solutions. The World.

The GVF Product Security Baseline

Current Status: GVF PSB is released!

Task Force members have access to the specification, and are starting implementation, since we do not know when vulnerabilities will be detailed or exploited.

Successful implementation requires a “culture of security,” may not be easy (or cheap) – but it does need to happen.

GVF Satellite. Solutions. The World.

Wrapping up…

In conclusion: This isn't going away.

Security scrutiny of the satellite industry is higher than it's ever been.

Exploitation of systems is widely discussed, and we should assume the bad guys are paying attention too – and using that knowledge maliciously.

GVF Security Task Force – a coordination center for satellite security knowledge

Vendors and network operators should implement robust protection, abandon widely discredited practices where they still exist.

Now - **Satellite Service Provider Security Document (SSPSec)**

GVF Satellite. Solutions. The World.

Thank you.

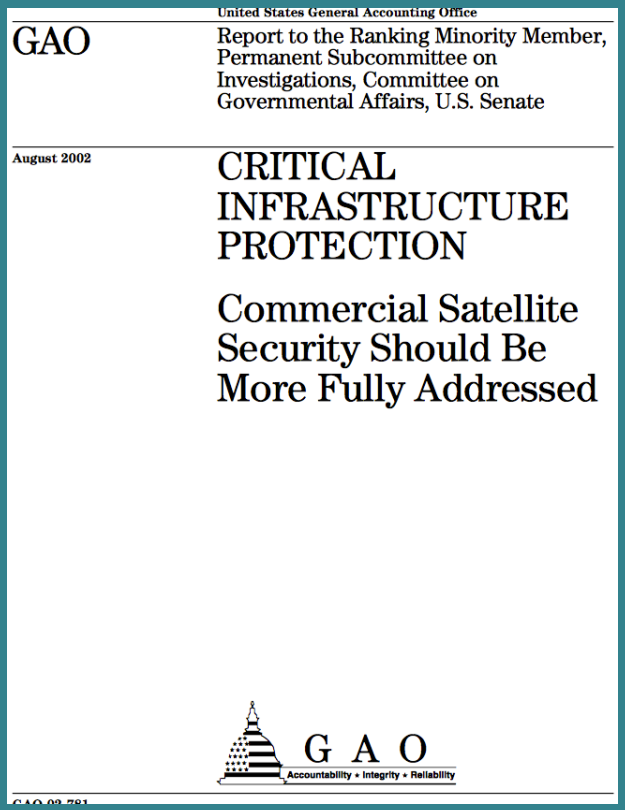
Backup Slides

Because we have been here before…

GAO Report, August 2002

"Commercial Satellite Security Should Be More Fully Addressed"

"Commercial satellite service providers have established operational procedures, including security techniques, some of which, according to officials, cannot be easily changed."



United States General Accounting Office

GAO

Report to the Ranking Minority Member, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate

August 2002

CRITICAL INFRASTRUCTURE PROTECTION

Commercial Satellite Security Should Be More Fully Addressed

GAO

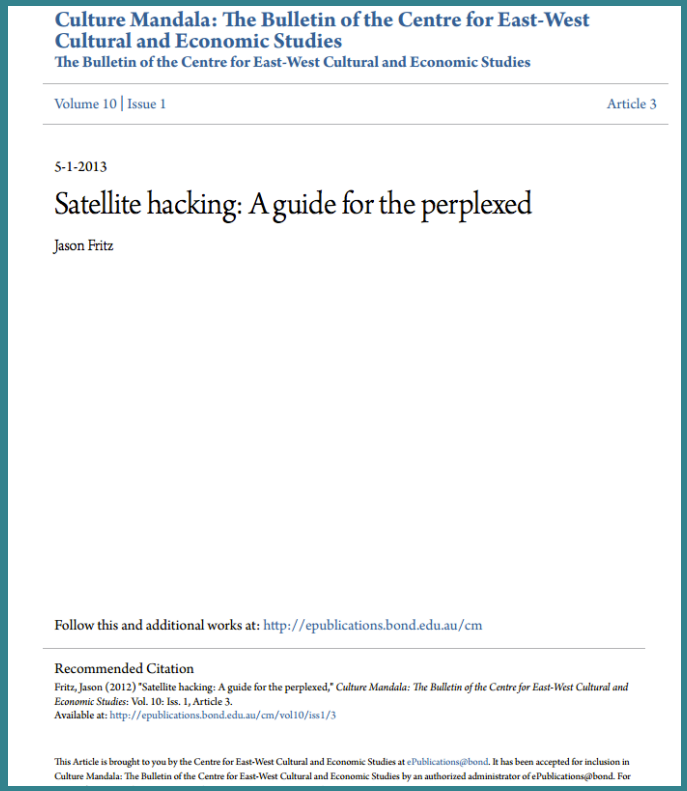
Accountability • Integrity • Reliability

Because we have been here before…

"Satellite Hacking, a Guide for the Perplexed" (May 2013)

"A root cause of many satellite vulnerabilities is an attempt to cut cost…

profit driven risk assessment, particularly with commercial operators, has resulted in increased Internet connectivity and reduced redundancy, hardening, and encryption. Increasing Internet connectivity of satellite systems increases performance and reduces the cost of operations, but it exposes satellite systems to increased risk of malicious activity."



Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies
The Bulletin of the Centre for East-West Cultural and Economic Studies

Volume 10 | Issue 1 Article 3

5-1-2013

Satellite hacking: A guide for the perplexed

Jason Fritz

http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1131&context=cm