ICS-CERT ADVISORY

ICSA-10-316-01A—INTELLICOM NETBITER WEBSCADA MULTIPLE VULNERABILITIES

UPDATE A

December 16, 2010

OVERVIEW

On October 1, 2010, independent researchers identified vulnerabilities in the IntelliCom Netbiter Supervisory Control and Data Acquisition (SCADA) applications. A directory traversal vulnerability that can lead to local file disclosure is present in all affected devices. The ability to upload malicious web content using a custom logo page is also possible. All the reported vulnerabilities require superadmin privileges. If the default password is not changed, the vulnerability can be leveraged to gain additional access to an affected device's file system.

--------- Begin Update A--------

Intellicom has released a software update that limits the ability to read system files and eliminates the ability to perform directory traversals.

--------- End Update A--------

AFFECTED PRODUCTS

IntelliCom Netbiter products based on the NB100 and NB200 platforms, including:

- WebSCADA (WS100)
- WebSCADA (WS200)
- Easy Connect (EC150)
- Modbus RTU – TCP Gateway (MB100)
- Serial Ethernet Server (SS100)

IMPACT

A user with superadmin privileges (highest authentication level) has permission to read system files. Local configuration files can be accessed that may allow an attacker to research other potential attack vectors. The risk also exists for an attacker to execute arbitrary commands by uploading malicious code.

Impact to individual organizations depends on many factors that are unique to each organization. The ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

BACKGROUND

According to their website,[1] IntelliCom NetBiter products have been deployed in over 40 countries. NetBiter products are used to manage power generation applications and have been used with a number of generator sets/control panels.

The markets for NetBiter products include:

- Industrial automation
- Power generation
- Energy management
- Building automation
- Asset management.

NetBiter webSCADA is an industrial gateway that gives equipment remote connectivity via Ethernet, Internet, local area networks (LANs), Telephone modems, Global System for Mobile Communications (GSM), and General Packet Radio Service (GPRS) networks.

The EasyConnect product is a remote device management product. It supports automation integration with the online server through web-based management of remote sites.

The Modbus Remote Terminal Unit (RTU)-Transmission Control Protocol (TCP) Gateway (MB100) connects serial Modbus products to SCADA software or Ethernet-based programmable logic controllers (PLCs) over Ethernet LANs. The gateway acts as a transparent connection between serial Modbus products and the standard Ethernet protocol Modbus TCP.

Netbiter Serial Ethernet Server (SS100) connects serial products over Ethernet or the Internet to a remote application. The Serial Ethernet Server encapsulates serial data (RS232 + RS485) into packets and transports it over Ethernet. The data can be transmitted in both directions, making it possible to access, manage, and configure remote equipment over LANs or the Internet.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

A user who has been authenticated at the superadmin level (highest authentication level) has permission to read system files by calling read.cgi with options to read a system file. Local configuration files may be accessed by exploiting a directory traversal vulnerability. This may lead an attacker to research other potential attack vectors. An attacker may also execute arbitrary commands by uploading malicious code.

VULNERABILITY DETAILS

1. IntelliCom, http://intellicom.se/, web site last accessed November 9, 2010.

EXPLOITABILITY

Exploitation of these vulnerabilities requires superadmin privileges. While malicious code may be uploaded via the logo upload page, it would be easier to enable the ftp server to transfer malicious files.

All these exploitable functions duplicate legitimate operations that are allowed by users with superadmin privileges.

Because superadmin privileges are required, caution should be exercised to avoid the use of default usernames and passwords. The exploitation of default user names and passwords to obtain superadmin access is a simple task requiring little skill.

EXISTENCE OF EXPLOIT

Access to a user account with superadmin privileges is all that is required for exploitation.

DIFFICULTY

All vulnerabilities identified in the researcher's report require authentication with superadmin privileges. If this is accomplished because an installation has not changed the default username and password, then exploitation may be a simple task requiring a low level of skill.

MITIGATION

IntelliCom has released a security patch for the WS100 and WS200 products that limits the ability to read system files and the ability to perform directory traversals.

RECOMMENDATIONS

The default user in Netbiter products has superadmin privileges. IntelliCom strongly recommends that customers change the default password immediately when commissioning the product. In addition, ICS-CERT advises customers to provide only the necessary privileges to users of the product (least privileges mode of operation). Other recommendations include:

--------- Begin Update A--------

- IntelliCom recommends[2] that users of the WS100/WS200 products apply the following patch: "ISFR-4404-0010.npb" available from http://support.intellicom.se

--------- End Update A--------

- Place all control systems assets behind firewalls and isolated from the business network and the Internet.
- Deploy secure remote access methods such as Virtual Private Networks (VPNs) for remote access.
- Remove, disable, or rename any default system accounts (where possible).

2. IntelliCom, IntelliCom Security Bulletin - ISFR-4404-0010- Information, website last accessed December 15, 2010.

- Implement account lockout policies to reduce the risk from brute forcing attempts.
- Implement policies requiring the use of strong passwords.[3]
- Monitor the creation of administrator level accounts by third-party vendors.

Organizations should follow their established internal procedures if any suspected malicious activity is observed and report their findings to ICS-CERT for tracking and correlation against other incidents. ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures.

The Control System Security Program provides numerous recommended practices[4] for control systems on the US-CERT website. Several relevant recommended practices are available for reading or downloading, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585

For Control System Security Program Information and Incident Reporting:
www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

3. NIST, http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf, web site last accessed November 5, 2010.
4. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, web site last accessed January 12, 2010.