ICS-CERT ALERT

ICS-ALERT-10-293-01 - MULTIPLE VULNERABILITIES IN INTELLICOM NETBITER WEBSCADA
October 20, 2010

ALERT

SUMMARY

Russian firm ITDefense has reported multiple vulnerabilities in Intellicom's Netbiter® WebSCADA product.

According to IntelliCom, their NetBiter® products have been deployed in over 40 countries. The markets for NetBiter® solutions include industrial automation, power generation, energy management, building automation, and asset management.

The three issues identified by ITDefense all appear to be related to a directory traversal vulnerability that can be exploited through the WebSCADA embedded web server. If a user has been authenticated with "superadmin" privileges, (highest authentication level) they have permission to read system files by calling read.cgi with options to read a system file.

ICS-CERT is working with Intellicom to address these vulnerabilities. As an interim mitigation, Intellicom recommends customers change the default password when installing the product. In addition, they strongly advise customers to provide only the necessary privileges to non-administrator users of the product.

ICS-CERT will provide additional information as it becomes available.

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT.

Other resources:

http://seclists.org/bugtraq/2010/Oct/1

http://secunia.com/advisories/41671/

ICS-CERT Operations Center
1-877-776-7585
www.ics-cert.org
ICS-CERT@DHS.GOV

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.