NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Industry Advisory

Telephony-Enabled Weakness

Initial Distribution: August 2, 2011

Current status of threat/vulnerability

[Why am I receiving this? >>]
[About NERC Alerts >>]

Status:	No Reporting is Required – For Information Only
	**Public:** No Restrictions. Will be posted to NERC's website alert page. [More on handling >>]
Instructions:	NERC Advisories are designed to improve reliability by disseminating critical reliability information and are made available pursuant to Rule 810 of NERC's Rules of Procedure, for such use as your organization deems appropriate. **No particular response is necessary.** This NERC Advisory is not the same as a reliability standard, and your organization will not be subject to penalties for a failure to implement this Advisory. Additionally, issuance of this Advisory does not lower or otherwise alter the requirements of any approved Reliability Standard, or excuse the prior failure to follow the practices discussed in the Advisory if such failure constitutes a violation of a Reliability Standard.
Distribution:	**Initial Distribution:** Reliability Coordinator, Transmission Owner, Transmission Operator, Balancing Authority, Generation Owner, Generation Operator, Distribution Provider, Load-Serving Entity, Transmission Service Provider. [Who else will get this alert? >>] [What are my responsibilities? >>]
Primary Interest Groups:	EMS Administrators, GMS Administrators, Cybersecurity – Control Systems, Cybersecurity – Corporate IT, System Administrators.
Advisory:	The ES-ISAC was recently contacted by a security researcher who has discovered a potentially broad vulnerability where cellular messaging is used to attack embedded systems architecture control networks. Clear text messaging protocols can be intercepted and reverse engineered to enable an attacker to inject commands or implement attacks on critical systems which rely on embedded microprocessors. Impacts could include breach of physical security perimeters or malicious manipulation of Bulk Power Control Systems. TCP/IP or SMS blast attacks to many random IP addresses, or targeted attacks could be launched either in close proximity to control devices or from external points on the telephony network. Some microprocessors in use within selected Bulk Power System (BPS) control networks or physical security perimeter control networks today may have cellular signal reception capability but do not have adequate application space or CPU speeds to assure message confidentiality, integrity, or guarantee of origin. For this reason, attackers can inject malicious commands towards unsecured end points. The security researcher has indicated that these vulnerabilities potentially extend to any architecture dependent on chipset embedded application processors and subject to cellular intercept where target control system networks utilize unsecured end points. It is important for entities to understand where their BPS control systems network environment and equipment inventory includes embedded microprocessors and microcontrollers potentially subject to cellular intercept. It is also increasingly important to maintain keen awareness of advancing technical knowledge regarding this vulnerability.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Background:	Proprietary control systems network environments, third party servicing architectures and remote access regimes have become increasingly reliant on embedded systems architectures utilizing application processor microcontrollers with cellular signal receipt capability. These architectures are potentially subject to messaging security vulnerabilities. Physical perimeter security breach and control system attack are possible impacts. Security researchers have demonstrated engineering attack methods which can result in control systems microprocessor and network vulnerabilities. While many specific chipsets and architectures exist, they may share broad collective and individual vulnerabilities. Awareness of this potential emerging vulnerability indicates the need to better understand the scale and nature of reliance on these technologies. Understanding the specifics of cellular communications pathways, uses and potential security exposures proximate to control microprocessors within your network environment carries increasing importance. It also underscores the current importance of careful attention to new developments in potential attack techniques, tactics, and related mitigation strategies.
Mitigation Options	• Entities should consider where in their environments this cellular enabled technology exists and if any mitigation should be considered based on this newly discovered exploit. (Network Architecture-Root Cause Analysis-RCA) • Entities should work with device vendors to better understand the scale and character of current reliance on vulnerable architectures, prospective requirements for, or security benefits of, encryption processor or hardened proprietary application/protocols. (Vendor Collaboration) • Activation of embedded feature sets which enable message filtering, private cloud network provisioning, or layered VPN with selected IPSEC device addition could provide added security in some cases. Establishment of a SCADA frontier to field firewall IPSEC or SSL VPN tunnel to carry control instructions could also provide mitigation. (Feature Set Activation) • Entities should consider when equipment upgrade opportunities occur to upgrade to technology that supports encryption or implement serial based encryption hardware that interfaces with identified high risk devices. (Supply Chain Mitigation) • Entities should consider the security viability and impacts of specific cellular communications mediums very carefully, especially cellular communications cards which rack into PLC/RTU backplanes or snap directly to the controller. Be aware that this architecture may place control devices on these backplanes within a foreign network or create new potential attack surfaces. (Cyber Security Risk Assessment) • Entities should consider participation in a future NERC webinar focused on this topic. Notice will be posted on the ES-ISAC web page at www.esisac.com . (Training & Awareness)
Contact:	Tim Roxey Director of Critical Infrastructure Risk Management and Technology Division North American Electric Reliability Corporation (NERC) 1120 G Street NW, Suite 990 Washington, DC 20005 Telephone: (202) 400-3013 Fax: (202) 393-3955 Tim.Roxey@nerc.net To report any incidents related to this Advisory, contact: ES-ISAC 24-hour hotline 609.452.1422 esisac@nerc.com
Attachment	Telephony-Enabled Weakness description

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com