NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Industry Advisory

Two-Factor Authentication Compromise

Initial Distribution: April 4, 2011

Increased Threats to Authentication Services

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: Primary Compliance Contacts** Reliability Coordinator, Transmission Owner, Transmission Operator, Balancing Authority, Generation Owner, Generation Operator, Distribution Provider. Who else will get this alert? >> What are my responsibilities? >>
Primary Interest Groups:	Cyber Security – Control Systems, Cyber Security – Corporate IT, System Administrators, EMS Administrators, GMS Administrators, RSA Administrators
Advisory:	NERC has confirmed with RSA the recent cyber attack on SecurID two-factor authentication products. This attack may affect the security of the two-factor authentication tokens from RSA used by industry to allow remote access to entity devices and systems. Although the extent of the cyber attack on RSA is unknown, enough information may have been obtained by the attacker to allow a less sophisticated attack such as social engineering to succeed. The concern now is focused on information systems administration and user education steps that should be taken to help detect or prevent potential attackers from acquiring additional information from users. NERC is encouraging entities to implement the mitigation strategies outlined in Attachment 1 of this Advisory. This attachment contains specific information and suggested actions for mitigation in accordance with standard

detection, prevention, and recovery phases of an effective incident response and cybersecurity program.

NERC is further encouraging entities to carefully review the Early Warning and Indicator Notice (EWIN)-11-077-01A Update that is attached to the Alert and take appropriate actions as described in Attachment 1.

Since RSA has confirmed that specific information related to SecurID two-factor authentication products was compromised with the extent of the compromise unknown, the ES-ISAC estimates the potential risk to bulk power system reliability from this attack is **MEDIUM**.

Attached:
Attachment 1 – Mitigation Measures for Two Factor Authentication Compromise
Attachment 2 – Early Warning and Indicator Notice (EWIN)-11-077-01A UPDATE

Background:

On March 17, 2011, RSA announced that a cyber attack on its systems was successful and resulted in the compromise and disclosure of information "specifically related to RSA's SecurID two-factor authentication products." While the full extent of the breach remains unconfirmed, RSA states that "this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack." Enough information may have been obtained by the attacker to facilitate successful spearphishing or social engineering attacks.

Attachment 1 provides specific actions for consideration by IT administrators and end user communities. Possible attack vectors include:

1. RSA Seed Record Compromise – A seed record is a shared secret between a hardware authenticator (e.g. token) and the authentication server. These seed records are commonly, but not always, used in combination with a user generated Personal Identification Number (PIN). Compromise of the seed code could potentially allow duplicate token values to be generated without possession of the token requiring only the guessing of the Users PIN, if a PIN had been used, to achieve full compromise and potential subsequent access.

2. Social engineering – Social engineering attacks trick users into performing an act that provides the attacker with confidential information. Depending on the nature of the information that was compromised from RSA, social engineering could be used to obtain the missing information necessary for the adversary to guess a Users PIN or might even trick the User into giving their PIN directly to the attacker.

Although an old technique, social engineering attacks are still effective and end user training is critical for reminding users to be wary of such attacks and to report suspicious events.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Contact: Steve Applegate
Cyber Security Threat and Vulnerability Program Manager
North American Electric Reliability Corporation (NERC)
1120 G Street NW, Suite 990
Washington, DC 20005
Telephone: (202) 503-7192
Fax: (202) 393-3955
Steven.Applegate@nerc.net

To report any incidents related to this Advisory, contact:
ES-ISAC 24-hour hotline
609.452.1422
esisac@nerc.com

A-2011-04-04-01