NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Attachment 1 – Mitigation Measures for Two Factor Authentication Compromise

Potential Impacts

Specific details regarding the nature of a possible attack exploiting RSA SecurID two-factor authentication products have not been publicly released. Therefore, any actionable mitigation must presume the total loss of confidence in all remote authentication mechanisms.
Depending on the nature of the information 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.

Disclosure of the following categories of information could prove valuable to a would-be attacker seeking to launch an attack exploiting this type of failure:

- Seed Records used in hardware or software tokens manufactured to date.
- Relationship of those seeds to specific token serial numbers.
- Relationship of seeds or token serial numbers to specific clients.
- Information regarding the RSA SecurID algorithm which could expose mathematical and cryptographic weaknesses.
- Information regarding specific implementations of the algorithm that might reveal implementation weaknesses in specific products.
- Source code or other information regarding ACE servers[1] that might reveal vulnerabilities.

Basic Mitigations for System Administration Personnel

Affected entities should consider the following mitigation measures as general security practices that reduce the effectiveness of an attack using compromised RSA information:

- Carefully review the Early Warning and Indicator Notice (EWIN)-11-077-01A Update that is attached to the Alert. Add malicious domains to router access control lists or other security hardware as applicable.
- Review all user remote access requirements and revoke any deemed non-essential.
- Establish a lockout threshold (e.g. three to five) for failed login attempts and require user interaction to re-launch the login process and perform a log review. This mitigation thwarts an automated, brute-force attack which would be trivial for guessing the typical four character numeric PIN.
    - Increase PIN security: if no PIN is used, explore a solution that employs one; if the PIN in use is numeric only, explore ways to increase complexity; recommend following RSA’s Best Practices Security Guide for PIN security. Additionally, require an immediate PIN change for all RSA SecurID authenticated accounts.
- Disable the remote access infrastructure when not in use.

[1] RSA ACE/Server® software is the management component of the RSA SecurID® solution, used to verify authentication requests and centrally administer authentication policies for enterprise networks.

- Take measures to implement more robust system configurations and awareness with IT support staff to include:
  - Enable verbose logging for all centralized authentication services and collect the IP address of the system accessing the service, the username and the resource accessed, and whether the attempt was successful or not.
  - Counter brute-force attacks attempting to determine the specific PIN used for a given account's SecurID token by monitoring for repeated authentication failures on both the ACE server and intermediate appliances and systems; conduct near real-time log review for passed and failed attempts per user and per unit of time independent of successful logins and lockouts.
  - Be aware of staff behavioral anomalies such as increased or excessive outbound traffic (e.g. email) and activity outside normal working hours. Compare with historic usage.
  - Deploy a SIEM (Security Information and Event Management) solution with event correlation.
- Mitigate direct attacks against ACE servers by hardening the server, implementing host-based security controls, and maintaining a robust change management scheme to ensure security patches are up to date. Contact vendor for specific hardening techniques, which may be unique to the ACE server.
- Implement recommendations as outlined in US-CERT TIP-11-075-01. (http://www.us-cert.gov/reading_room/TIP11-075-01.pdf)
- Carefully review all available information in the US-CERT member's area and if necessary, join the US-CERT portal. (http://www.us-cert.gov)

Enhanced Protection Measures for System Administration Personnel

Affected entities should consider the following enhanced mitigation measures:

- Contact the vendor for additional best practices and company specific information.
- Add additional levels of authentication such as a third factor.
- Monitor for changes in source of authentication attempts and multiple concurrent logins for a single account.
- Restrict access by IP and MAC address wherever possible.
- Limit concurrent logins to one per user.
- Apply additional defense-in-depth techniques.
- Enable defenses against key-logging such as forced frequent credential changing and updated anti-virus (AV) signatures.
- Validate software by requiring validation of vendor-provided hash values or digital signatures prior to installation. If information is not customarily provided, request validation guidance from the vendor.
- Establish installation baseline (e.g., file names, versions, hash values) and periodically revalidate this information. Prior to baseline, the system should be confirmed as secure and clean of malicious software to avoid the baseline of a compromised system.
- Suspend the practice of providing emergency-code tokens.
- Immediately address all reports of lost or stolen tokens.
- Enable revocation checking to include Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL) checking.

- Educate users' expectations as to which systems prompt for One Time Passwords (OTP) to protect against phishing and social engineering attempts.
- Display recent attempted login attempts to a user on login.

Protection Measures for End Users

End Users of IT and control systems should consider the following mitigation measures:

- PIN control measures such as:
  - Phishing that may seek to capture PINs.
  - DO NOT share your PIN with anyone.
  - DO NOT write PIN or any business identifying information on tokens.
- Token Control Measures:
  - DO NOT give the serial number of tokens to anyone other than verified entity support personnel.
  - Physically protect a token by carrying it with you or keeping it in a secure location at all times.
- User personnel should be suspicious of unsolicited phone calls, e-mail messages or other communications from individuals or businesses that ask about an entities' organization structure, personnel, financial information or operations.
- DO NOT access unsolicited web links received in e-mail messages or faxes.
- DO NOT respond to unsolicited faxes, pop-up windows or advertisements online, via email or text.

Cyber Event or Incident Reporting

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

Reference Information

Open Letter to RSA Customers:
http://www.rsa.com/node.aspx?id=3872

Form 8-K filing with SEC:
http://www.sec.gov/Archives/edgar/data/790070/000119312511070159/d8k.htm

RSA SecurCare Online Note:
http://www.sec.gov/Archives/edgar/data/790070/000119312511070159/dex992.htm

The RSA SecurCare Online and security best practices guides is:
http://www.rsa.com/path/docs/pdfs.zip