Date: 18 March 2011

Rapid Release IA Alert: (U) This issuance is released under the “Rapid Approval and Release Process”. This issuance is used to release time sensitive information to U.S. customers and will be followed by a formal IA Advisory.

SUBJECT: (U) Mitigations for the RSA Cyber Intrusion

1. (U) On 17 March, RSA announced that it had been the victim of a cyber intrusion. In that message, the company revealed that information related to SecureID, a leading two-factor authentication product, had been taken from its network. Furthermore, the company claimed that the compromise does not lead to a direct attack on the product but does decrease its effectiveness. Because authentication products are used to assure that only authorized personnel are able to access protected resources, being able to successfully exploit this situation could allow an unauthorized user to masquerade as a legitimate user and thus access those protected resources.

2. (U) Additionally, RSA released information, to include proposed mitigations, via its RSA SecureCare Online web portal. The NSA recommends that customers with access to that portal review and consider implementing those recommendations.

3. (U) Based on NSA’s experience with two-factor authentication, it does not appear that the compromise leads to a direct attack on SecureID but that it does lessen the level of security provided by the product. The extent to which the security is decreased may vary greatly from customer to customer so a single impact statement cannot be issued.

4. (U) In response to this, the DHS issued the “Technical Information Paper – TIP-11-075-01 System Integrity Best Practices” (http://www.us-cert.gov/reading_room/TIP11-075-01.pdf). This TIP calls for end-users to:
   - Enable strong logging,
   - Limit remote access,
   - Apply additional defense-in-depth techniques, and
   - Validate software.

The TIP specifies additional detailed information so the NSA recommends that customers review it and consider implementing those recommendations.

5. (U) In addition to the above recommendations, the NSA would like to recommend the following:
Reset each user’s PIN. If possible, do this via a face-to-face meeting with the token’s owner. This could also be used as an opportunity to review logs for that user in an attempt to find unauthorized accesses.

Administrators should limit the ability to remotely access the network to only those users needing remote access to perform official duties. This should not be a standard access for all users.

Alert users to the potential of receiving phishing emails asking them to enter information specific to that user, such as PIN, username, password, tokencode, passcode, or token serial number, which is found on the back of the token.

6. (U) The NSA recommends that users take basic steps to harden their infrastructures so that they are less vulnerable to network intrusions. The Information Assurance portion of the NSA’s internet website contains configuration guidance and best practices on a wide range of topics. The following two documents specifically provide recommendations on means to defend against two of the more prevalent web threats:

   - (U) Mitigation Monday – Defense Against Malicious E-mail Attachments
     http://www.nsa.gov/ia/_files/factsheets/MitigationMonday.pdf

   - (U) Mitigation Monday #2 – Defense Against Drive-By Downloads

7. (U) The NSA will continue to work this situation and will provide additional information and guidance, as needed.

8. (U) Questions concerning this Advisory should be directed to the NSA Information Assurance Customer Advocate Office at 410-854-4790.

Tony Sager
Chief, Vulnerability Analysis and Operations