



**Centre for Critical Infrastructure Protection
Threat Information Product (TIP)**

Mitigations Following RSA Security Breach

Serial Number: CCIP-TIP_UA6A110323-01

Date: Wednesday 23rd March 2011

This information must be handled in accordance with the above Traffic Light Protocol (TLP)¹ handling caveat.

Summary:

Following the security breach affecting RSA SecurID two factor authentication products, CCIP would like to draw your attention to some potential mitigations.

Degree of Credibility:

Extremely Credible

Breach confirmed by Vendor.

Impact Criticality:

Highly Critical (TBC)

Full extent and impact TBC.

Level of Verification:

Confirmed

Confirmed by Vendor.

Availability of Exploit:

N/A

Assessed that information extracted does not enable a successful direct attack, however; information could be used to reduce the effectiveness of a current two-factor authentication.

Solution:

CCIP recommends the following mitigations:

- **Strengthen defence-in-depth techniques:**
 - Reset each users personal identification number (PIN).
 - Maximize complexity of passwords, passphrases, and PINs.
 - Enable defences against key logging such as forced frequent credential changing and updated anti-virus (AV) signatures.

¹ For a definition of the TLP please contact CCIP or see the following link:

<http://www.ccip.govt.nz/incidents/tlp.html>



- **Limit remote access:**
 - Reduce remote access to just those users requiring it.
 - Restrict access by IP address wherever possible.
 - Limit a user's concurrent logins to one per user.
- **Advice for users:**
 - Remind users to never give the token serial number, PIN, tokencode, token, passcode or passwords to anyone.
 - To avoid phishing attacks, do not enter tokencodes into links that you clicked in e-mail. Instead, type in the URL of the reputable site to which you want to authenticate.
 - Tell your users what information requests to expect from Help Desk administrators (and ensure this process is not at risk of a socially engineered attack) .
- **Enable strong logging:**
 - Enable logging for all centralized authentication services and collect the IP address of the system accessing the service, the username, the resource accessed, and whether the attempt was successful or not.
 - Limit the number of authentication attempts and lockout the user if the limit is reached. If possible, security professionals should conduct a manual review before unlocking the account and prohibit automatic unlocks after a specified time period.
 - Conduct near real-time log review for failed attempts per user and per unit of time independent of successful logins; abnormal successful logins; and lockouts. Correlate this data to identify anomalous activity.
 - If possible, engage individually with users to review their access logs in an attempt to find unauthorized access.
- **Monitor the situation:**
 - CCIP also strongly advises RSA SecurID customers to remain engaged with RSA and apply recommendations from them.
 - Implement security hardening advice as detailed in the *RSA SecurID Authentication Engine Best Practices Guide*.
 - Monitor the IT Security related News for emerging issues.

Handling Caveat: **GREEN**

File Note: 95/1 0004-01



Discussion:

CCIP would welcome any feed back or comments on this product. If you should be targeted by an attack please report it to CCIP. As and when CCIP becomes aware of any further relevant information we will update this alert.

Links:

<http://www.rsa.com/node.aspx?id=3872>

http://www.us-cert.gov/reading_room/TIP11-075-01.pdf

Handling Caveat: **GREEN**

PO Box 12-209, Wellington, New Zealand • phone: +64 4 498 7654 • fax: +64 4 498 7655 • email: info@ccip.govt.nz

While this publication is accurate to the best of our knowledge, CCIP does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. CCIP will not be liable for any loss or damage howsoever caused, arising from or in connection with the use of information contained in this publication.

Reference in this publication in any manner to any commercial product, process or service does not constitute or imply its endorsement or recommendation by CCIP. Views and opinions in this publication herein may not be used for advertising or product endorsement purposes.