NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY

RSA SECURID TOKEN AUTHENTICATION AGENT VULNERABILITIES

DISCUSSION

A recent error handling vulnerability has been discovered in two RSA®[1] (Rivest Shamir Adleman) Authentication Agent toolkits and in one Authentication Agent product. This vulnerability can result in authentication bypass and affects a limited number of applications. These toolkits and product are used to deploy RSA SecurID Token Authentication to authenticate users to workstations, web servers, and network devices.

The RSA Authentication Agent Software Development Kit (SDK) for C version 8.5 and RSA Authentication Agent API for C version 8.6 contain this vulnerability.[2,3] Vulnerable implementations include custom deployments based on these SDK/API versions in Transmission Control Protocol (TCP) asynchronous mode. The vulnerability was also found in the RSA Authentication Agent for Web used in versions of the Apache Web Server[4,5]: Apache Web Server 8.0 and Apache Web Server version 8.0.1 prior to Build 618.

These products may have been deployed in the last two years. Systems utilizing either of the affected products are potentially vulnerable and should be updated immediately.

MITIGATION ACTIONS

Continued use of affected RSA Authentication Agent API and SDK implementations exposes systems to high risks of unauthorized access. Upgrade to the newest versions of RSA Authentication Agent API/SDK and implement according to RSA guidelines.[6,7] If a system administrator is unsure if their system is vulnerable or needs additional support, contact RSA representative or call the RSA Software Technical Support at 1-800-995-5095.

For systems operating susceptible RSA Authentication Agent for Web for Apache Web Server products, upgrade to Apache Web Server version 8.0.1 Build 618 or later versions.[8]

TECHNICAL ADDENDUM

To determine if a system is vulnerable, locate the SecurID Agent Authentication library file and determine the file's version number. The version of the aceclnt.dll file is the same as the version of the SDK/API used in the system implementation. For Windows machines, the library file is named aceclnt.dll, while on Unix machines, it is named libaceclnt.dll.

- For Windows devices, the version number can be determined by right clicking the file, selecting properties, and clicking the details tab. If the file location is unknown, search aceclnt.dll in C:\\ in Windows File Explorer.

---

[1] RSA is a registered trademark of RSA Security LLC

[2] CVE-2017-14378: https://nvd.nist.gov/vuln/detail/CVE-2017-14378

[3] ESA-2017-146: seclists.org/fulldisclosure/2017/Nov/48

[4] CVE-2017-14377: https://nvd.nist.gov/vuln/detail/CVE-2017-14377

[5] ESA-2017-145: seclists.org//fulldisclosure/2017/Nov/46

[6] RSA Authentication Agent SDK for C version 8.6.1: https://community.rsa.com/docs/DOC-85036

[7] RSA Authentication Agent API for C version 8.5.1: https://community.rsa.com/docs/DOC-85038

[8] RSA Authentication Agent for Web: Apache Web Server version 8.0.1 Build 618: https://community.rsa.com/docs/DOC-85062

- For UNIX devices, the following string command can be executed.
  - $ strings <path to library> /libaceclnt.so | grep “Agent Version”
  - If the location of the file is unknown, execute the following find command in the root directory.
    - $ find –name aceclnt.dll

DISCLAIMER OF ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

CONTACT INFORMATION

For further information about this product, please contact:

Client Requirements and General Cybersecurity Inquiries

Cybersecurity Requirements Center

410-854-4200

Email: Cybersecurity_Requests@nsa.gov