NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY

RSA KEY GENERATION VULNERABILITY AFFECTING TRUSTED PLATFORM MODULES

DISCUSSION

A vulnerability in a cryptographic library used to generate Rivest-Shamir-Adleman (RSA®[1]) encryption keys was recently disclosed.[1] The vulnerability allows recovery of a private key when only possessing a public key.[2] The vulnerable library is included in the firmware of specific Infineon® Trusted Platform Modules[3] (TPMs) present in systems produced by a number of Original Equipment Manufacturers (OEMs) commonly used in the Department of Defense (DoD). Much of the published guidance focuses on Windows® but the vulnerability is not in Windows®. All systems and devices[4] that include or use the vulnerable library are affected.

MITIGATION ACTIONS

A custom Tenable™ Nessus® audit file and PowerShell™ script are available at http://www.github.com/iadgov/Detect-CVE-2017-15361-TPM to aid in identifying Windows® systems that have a vulnerable TPM enabled. Ensure all September and October 2017 Microsoft® Patch Tuesday patches are installed first. Install OEM-provided firmware updates that patch the vulnerable library. See Microsoft® security advisory ADV170012[5] to determine the correct actions to take for the various Windows® features and services that use a TPM. Clear and re-initialize the TPM to generate new keys.

ENDNOTES

[1] Information on software update of RSA key generation function.
https://www.infineon.com/cms/en/product/promopages/rsa-update

[2] Vulnerability Note VU#307015: Infineon RSA library does not properly generate RSA key pairs.
https://www.kb.cert.org/vuls/id/307015

[3] Information on TPM firmware update for Microsoft Windows systems.
https://www.infineon.com/cms/en/product/promopages/tpm-update

[4] Security Advisory 2017-10-16. https://www.yubico.com/support/security-advisories/ysa-2017-01

[5] ADV170012 | Vulnerability in TPM could allow Security Feature Bypass. https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV170012

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.

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

TRADEMARK INFORMATION

Infineon® is a registered trademark of Infineon Technologies AG. Microsoft®, Windows®, and PowerShell™ are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Nessus® is a registered trademark of Tenable, Inc. Tenable™ is a trademark of Tenable, Inc.

CONTACT INFORMATION

For further information about this product, please contact:

Cybersecurity Requirements Center

410-854-4200

Email: Cybersecurity_Requests@nsa.gov