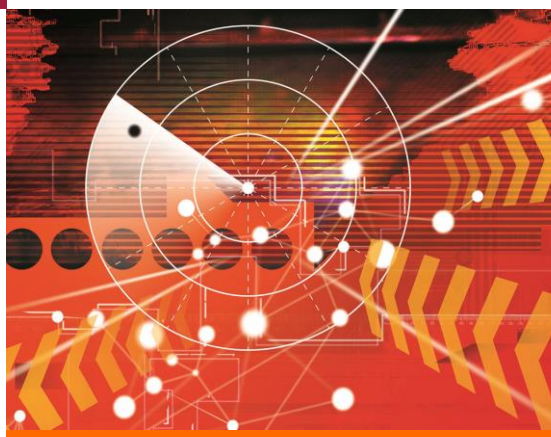
Infinion TPM-Breach ROCA (CVE-2017-15361)

Experience the commitment®

Aktuelle Sicherheitsinformation



Trusted Plattform Module sind quasi in Hardware gegossene Kryptographie und gelten als besonders sicher. Vor Design-Fehlern sind sie leider auch nicht geschützt, wie die Sicherheitslücke mit Kennung CVE-2017-15361 zeigt, die von ihren Entdeckern auf den Namen ROCA ("The Return of Coppersmith's Attack") getauft wurde.

DIE ATTACKE

Anfang des Jahres fanden Forscher des Centre for Research on Cryptography and Security in Tschechien einen Fehler in Infineons Implementation des RSA Algorithmus, der zum Erstellen kryptographischer Schlüsselpaare dient.

Dadurch kann aus dem öffentlich bekannten Teil des Schlüssels, dem sogenannten Public Key, der geheime Schlüssel errechnet werden. Zudem können öffentliche Schlüssel in wenigen Millisekunden automatisiert auf ihre Verwundbarkeit geprüft werden.

Das Problem wurde Infineon diskret mitgeteilt. Die Firma informierte alle betroffenen Kunden, darunter Microsoft, Google und Lenovo, und brachte am 10.10.2017 einen Patch für ihre Windows TPM Module heraus, bevor die Lücke am 15.10.2017 der breiten Öffentlichkeit bekannt wurde.

Das Problem exisitiert schon seit 2012.

DIE URSACHE

Die Implementation des Chipherstellers ist dafür verantwortlich, die für das Schlüsselpaar notwendigen Primzahlen zu liefern. Durch einen Fehler liefert der Algorithmus in unregelmäßigen Abständen schlechte Primzahlen aus, die die kryptographische Stärke der erzeugten Schlüssel beeinträchtigen.

2048 bit RSA Schlüssel können im Normalfall nicht im Zeitrahmen eines Menschenlebens geknackt werden. Durch den vorliegenden Angriff sind die betroffenen Schlüssel mittels Parallelisierung, hier im Beispiel durch eine Amazon AWS Instanz mit 1000 CPUs, schnell zu knacken.

- 512 bit RSA keys – 7,2 Sekunden – Kosten von 0.06$
- 1024 bit RSA keys – 2,3 Stunden – Kosten von $40-$80
- 2048 bit RSA keys – 51 Tage – Kosten von $20,000 - $40,000

FACT SHEET

INFINEON TPM CHIPS

Übersicht der Cybersecurity Lösungen:

Strategy, Compliance & Transformation

- Sicherheits- und Notfallmanagement
- Best Practices nach ISO 27001, ISO 25999, IT-Grundschutz und A-960/1
- Vulnerability Assessments und Penetration Testing
- Risikomanagementstrategien
- Aufbau von Sicherheitsprozessen
- Datenschutz und Datensicherheit
- EU-Datenschutzgrundverordnung
- Awareness Training

Secure Systems Engineering

- Sichere Netzarchitekturen
- Identity & Accessmanagement
- Sichere Softwareentwicklung
- Security Testing

Managed Security Services

- Managed Services
- Monitoring & Alerting
- SIEM as a Service
- Forensics & Malware Analysis
- Advanced Threat Intelligence

de.cgi.com/cybersecurity

DIE FOLGEN

Der überwiegende Teil der Hersteller hat bereits Sicherheitspatches herausgegeben, die eingespielt werden müssen. Fest verbaute Chips, z.B. in 750.000 Estnischen Personalausweisen, müssen in der Regel vollständig getauscht werden.

Betroffen sind nach derzeitigem Kenntnisstand Geräte folgender Hersteller:

- Microsoft
- Google
- HP
- Lenovo
- Fujitsu
- Yubi-Keys
- Diverse Smartcards

AD HOC GEGENMASSNAHMEN

Sollte ein betreffendes Gerät im Einsatz sein, so müssen alle Schlüssel die auf diesem erzeugt wurden, überprüft werden. Das Centre for Research on Cryptography and Security hat dafür eine Software veröffentlicht, die auf https://github.com/crocs-muni/roca heruntergeladen werden kann.

CGI berät Sie hierzu gerne, denn

“Cybersecurity is part of everything we do.”

Quellen:

https://crocs.fi.muni.cz/public/papers/rsa_ccs17

https://www.infineon.com/cms/en/product/promopages/rsa-update/rsa-background

https://arstechnica.com/information-technology/2017/10/crypto-failure-cripples-millions-of-high-security-keys-750k-estonian-ids/

https://support.hp.com/us-en/document/c05792935

https://support.lenovo.com/de/de/product_security/len-15552

http://www.fujitsu.com/global/support/products/software/security/products-f/ifsa-201701e.html

http://support.toshiba.com/sscontent?contentId=4015874

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV170012

https://nvd.nist.gov/vuln/detail/CVE-2017-15361

ÜBER CGI

Mit 70.000 Mitarbeitern an 400 Standorten in 40 Ländern übernimmt CGI vor Ort Verantwortung für den Erfolg seiner Kunden und bietet ihnen gleichzeitig globale Lieferfähigkeit. Seit unserer Gründung im Jahr 1976 pflegen wir eine strikte Lieferdisziplin, dank der unsere Projekte in Bezug auf Zeit- und Budgettreue in der Branche führend sind. Mit Business und IT Consulting, Systemintegration sowie Outsourcing Services auf höchstem Niveau unterstützt CGI seine Kunden dabei, laufende Investitionen besser zu nutzen und gleichzeitig neue Technologie- und Business-Strategien einzusetzen, mit denen sich optimale Lösungen für die gesamte Wertschöpfungskette erreichen lassen.

Das Resultat unseres Commitments zeigt sich im gemessenen Kundenzufriedenheitswert, der in den vergangenen zehn Jahren durchgängig mehr als 9 von 10 möglichen Punkten betrug.

IHR ANSPRECHPARTNER

CGI Deutschland Ltd. & Co. KG

Practice Cybersecurity

(Practice Head: **Frank Reiländer**)

Ettore-Bugatti-Straße 6-14
51149 Köln
T: +49 2203 6993 1050

Für weitere Informationen kontaktieren Sie uns unter csi@cgi.com
oder besuchen Sie uns auf de.cgi.com/cybersecurity.