P R E S S E M I T T E I L U N G

(ca. 50 Zeichen pro Zeile)

MTG entdeckt Sicherheitslücke bei CMS- und PKCS#7-Signaturen

Darmstadt, 30.11.2023 – **Am 22. Oktober veröffentlichte die Darmstädter MTG AG ein Papier, der einen Bericht über eine bisher nicht bekannte prinzipielle kryptographische Schwachstelle in den Protokollen CMS (Cryptographic Message Syntax) und PKCS#7 (Public Key Cryptography Standard) enthielt.**

Ein Sicherheitsexperte des langjährigen Spezialisten für PKI (Public Key Infrastructure) hat eine grundsätzliche Sicherheitslücke in den Protokollen CMS und PKCS#7-Signaturen entdeckt. Und zwar stellt unter bestimmten Umständen die gültige Signatur über die eigentlich signierten Daten hinaus gleichzeitig eine gültige Signatur für andere Daten dar, welche nie regulär signiert wurden. Die Form dieser Daten ist allerdings sehr unflexibel und der Angreifer hat darauf höchstens in einem geringen Umfang Einfluss. Dass ein bestimmtes reales System dadurch angreifbar wird, ist zwar im Allgemeinen sehr unwahrscheinlich ob der unflexiblen Form der fälschlich signierten Daten, kann aber aufgrund der weiten Verbreitung dieser Protokolle nicht gänzlich ausgeschlossen werden. Wer daher kein Risiko eingehen möchte und seine auf CMS bzw. PKCS#7-Signaturen basierenden Systeme gegen diese potentielle Schwachstelle absichern möchte, kann die im Papier „An Existential Forgery Vulnerability of CMS and PKCS#7 Signatures“ beschriebenen Gegenmaßnahmen umsetzen.

-/-

Paper der MTG AG zur Sicherheitslücke:

https://eprint.iacr.org/2023/1801.pdf

MTG-PM-Sicherheitslücke CMS und PKCS#7 Signaturen.docx
Darmstadt, 30. November 2023
Anzahl Wörter: 173
Anzahl Zeichen: 1.320 (inkl. Leerzeichen)

Zur weiteren Kenntnis der Redaktion:
Die MTG AG wurde 1995 gegründet und ist ein führender Spezialist für anspruchsvolle Verschlüsselungstechnologien „Made in Germany". MTG Enterprise Resource Security Lösungen, kurz ERS ®, vereinfachen und zentralisieren das Management kryptographischer Schlüssel und Identitäten über den kompletten Key Management Lifecycle. Dabei werden branchenspezifische Anforderungen von Unternehmen und öffentlichen Einrichtungen berücksichtigt. Das MTG ERS ® Produktangebot umfasst Certificate Lifecycle Management, Public Key Infrastrukturen, Key Management Systeme und Hardware Security Module. Es werden zudem Cloud-Lösungen für eine Managed Corporate PKI und die Verschlüsselung von virtuellen Maschinen von VMware angeboten. MTG kooperiert regelmäßig mit Partnern aus Industrie und Wissenschaft in öffentlich geförderten Forschungsprojekten. MTG kooperiert regelmäßig mit Partnern aus Industrie und Wissenschaft in öffentlich geförderten Forschungsprojekten. Forschungsthema ist unter anderem die Post-Quantum-Kryptographie. So wurden bestehende MTG ERS® Komponenten um die PQC-Algorithmen CRYSTALS-Dilithium, Falcon und SPHINCS+ erweitert, um bereits heute Daten gegen zukünftige Angriffe durch Quantencomputer zu schützen. Alle Unternehmensprozesse bei MTG sind ISO 27001 zertifiziert.

Ihr Gesprächspartner:

Tamer Kemeröz
Vorstand MTG AG
Dolivostr. 11, 64293 Darmstadt
Telefon: 06151 / 8000-11
E-Mail: tamer.kemeroez@mtg.de
Internet: www.mtg.de

Ihr Partner Public Relations:

Dirk Roebers
PR Exclusiv – Dirk Roebers Public Relations
Rütger-von-Scheven-Str. 59e, 52349 Düren
Telefon: 02421/27 37 776
E-Mail: dr@pr-exclusiv.de
Internet: www.pr-exclusiv.de