



VOICE CSCC

Lagebericht zur IT-Sicherheit

datetime

16. März 2018

CSCC Case der Woche

Potenzielle Schwachstellen in AMD-Prozessoren

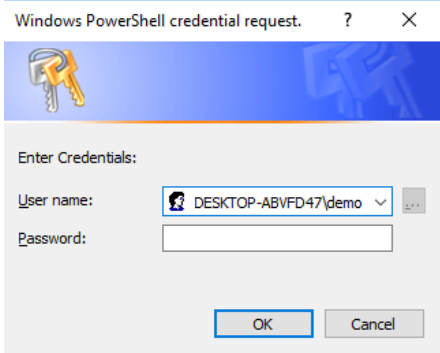
Title

		Risiko
		■■■□□
Sachstand:	<p>Sicherheitsforscher der CTS-Labs haben 13 Schwachstellen in AMD-Prozessoren identifiziert. Die Schwachstellen werden in vier Kategorien eingegliedert und ermöglichen diverse Angriffsszenarien:</p> <p>RYZENFALL: Code Execution, Bypass des Windows Credential Guard</p> <p>FALLOUT: Installation von persistenter Schadsoftware</p> <p>CHIMERA: zwei Backdoors (Firmware, Hardware)</p> <p>MASTERKEY: BIOS-Flashing, Installation von persistenter Schadsoftware.</p> <p>Die Schwachstellen sind praktisch in allen aktuell verbreiteten AMD-Systemen enthalten (EPYC Server, RYZEN Workstation, RYZEN Pro, RYZEN Mobile).</p>	
Bewertung:	<p>Die Medien stellen teilweise die Glaubhaftigkeit der Schwachstellen in Frage. Unter anderem wird dies dadurch begründet, dass die Firma CTS-Labs in der Security-Branche bisher unbekannt sei. Aus neutraler Sicht existieren im ersten Fall keine Beweggründe, von einer fälschlichen Sachlage auszugehen, zumal ein unabhängiger Dritter bereits einige der Schwachstellen bestätigt haben soll.</p> <p>Sollten die Schwachstellen seitens AMD bestätigt werden, hängt die Bedrohungslage zum einen von den aktuell noch unbekannten Angriffsvektoren und zum anderen von der Verbreitung der betroffenen Prozessoren statt. Naturgemäß wird die Situation mit Meltdown & Spectre verglichen, ein präziser Vergleich ist aufgrund noch nicht bekannten technischen Details aktuell nur schwer möglich.</p>	
Empfehlung:	<p>Zurzeit können keinen konkreten Empfehlungen ausgesprochen werden. Die gemeldeten Schwachstellen liegen AMD zur Überprüfung vor. Die Lage sollte weiter beobachtet werden.</p>	
Quellen:	<p>[1] Severe Security Advisory on AMD Processors</p>	

Details zur APT-Gruppierung „Inception Framework“

		Risiko ■■■■■
Sachstand:	<p>Symantec hat die Angriffsmethoden der Gruppe „Inception Framework“ analysiert. Inception Framework ist eine Gruppierung, die seit etwa 2014 aktiv ist und bereits mehrere erfolgreiche Spionage-Kampagnen durchgeführt hat.</p> <p>Eine der wesentlichen Fähigkeiten von Inception Framework ist die Verschleierung ihrer Identität. Durch kompromittierte Router werden kurzlebige Router-Kaskaden („Router“-Proxies) aufgebaut und ausspionierte Daten über verschiedene Wege transportiert.</p> <p>Der Infektionsweg geschieht per E-Mail über manipulierte Office-Anhänge, die Schwachstellen in der Microsoft Office Suite ausnutzen, zum Beispiel:</p> <ul style="list-style-type: none"> • CVE-2014-1761: Remote Code Execution durch manipulierte RTF-Dateien (CVSSv2: 9.3) • CVE-2012-0158: Remote Code Execution durch manipulierte RTF-Dateien, Webseiten oder Office-Dokument (CVSSv2: 9.3) <p>Inception Framework nutzt legitime Cloud-Anbieter, um die abgegriffenen Daten zu empfangen. Begonnen wurde mit einem Cloud-Anbieter, die Anzahl ist in den letzten Jahren stetig gewachsen.</p>	
Bewertung:	<p>Die Bedrohungslage durch APTs wurde im Rahmen des CSCC bereits mehrere Male bewertet. APTs stellen kontinuierlich eine hohe Bedrohungslage für Unternehmen dar. Abhängig vom Ziel und Zweck der APT (Spionage, Wiper etc.), der Branche des Unternehmens und der geographischen Ansiedlung können sich unterschiedliche Bedrohungslagen ergeben.</p> <p>Die Ausnutzung von bekannten Schwachstellen, die über Microsoft gepatcht werden, zeigt die Bedeutung eines wirksamen Patch-Management Prozesses. Gleichzeitig bedeuten eingespielte Sicherheitsupdates nicht zwangsläufig eine vollständige Sicherheit (diese existiert ohnehin nicht), sondern es muss davon ausgegangen werden, dass Gruppierungen wie Inception Framework über Zero-Day Exploits verfügen.</p>	
Empfehlung:	Um eine möglichst hohe Resistenz gegen APTs zu erreichen, müssen verschiedene Maßnahmen in einem größeren Maßnahmenverbund wirken („Defense-in-Depth“-Strategie).	
Quellen:	[1] Inception Framework: Alive and Well, and Hiding Behind Proxies	

PowerShell-Skript zum Diebstahl von Zugangsdaten

	Risiko ■□□□□
Sachstand:	<p>Aktuell wird von einem PowerShell-Skript gewarnt, welches das Ausspionieren von Zugangsdaten im Fokus hat. Das Skript basiert auf dem Commandlet (Cmdlet) „<i>Get-credential</i>“, welches das Standard-Eingabefenster von Windows öffnet und den Benutzer nach der Eingabe seines Benutzernamens und Passworts auffordert.</p>  <p>Abbildung 1: Interface des Get-Credential Cmdlet</p> <p>Daraufhin prüft das Skript die Zugangsdaten gegen einen Domain-Controller. Waren die Daten korrekt, werden diese an einen Server unter der Kontrolle des Angreifers übertragen, andernfalls erscheint das Fenster kurze Zeit später erneut. Mit diesem aufdringlichen Verhalten soll der Benutzer praktisch zu einer Eingabe seiner Daten gezwungen werden. Zudem lassen sich Titel und Nachricht in dem Cmdlet anpassen, sodass eine Nachricht wie „<i>Virus gefunden! Bitte geben Sie zur Bereinigung des Systems ihre Zugangsdaten ein!</i>“ in einer höheren Wahrscheinlichkeit für einen erfolgreichen Angriff resultieren können.</p> <p>Das permanente Auftreten der Eingabemaske lässt sich nur durch das Beenden des entsprechenden PowerShell-Prozesses im Task-Manager erreichen.</p>
Bewertung:	<p>Dieser Angriffstyp ist nicht neu, sondern ein klassischer Bestandteil der Post-Exploitation Phase (Phase, die nach erfolgreicher Ausnutzung einer Schwachstelle eintritt). Gängige Exploitation-Frameworks haben vorgefertigte Module zum Ausspionieren von Zugangsdaten integriert. Ein erfolgreiches Abgreifen der Zugangsdaten dürfte kein unrealistisches Szenario sein, die Herausforderung auf Seiten eines Angreifers besteht darin, das Skript auf einem Ziel-System zur Ausführung zu bringen.</p>
Empfehlung:	<p>Sowohl durch technische als auch organisatorische Methoden kann einem Angriff vorgebeugt werden. Technisch kann die Ausführung von PowerShell-Skripten (beispielsweise per Gruppenrichtlinien-Objekt) unterbunden werden. Organisatorisch können die Mitarbeiter eines Unternehmens sensibilisiert werden, zum Beispiel im Rahmen einer Warnung im Intranet. Auch wenn der Angriff nicht vollständig neu ist, verstärkt eine aktuelle Warnung das Bewusstsein eines</p>
Quellen:	<p>[1] PSA: Beware of Windows PowerShell Credential Request Prompts</p>

Kaspersky-Whitepaper zum Dark Web

		Risiko informativ
Sachstand:	<p>Kaspersky hat in einem kurzen Whitepaper einige Fakten zum Dark Web veröffentlicht.</p> <p>Neben einiger allgemeinen Erklärung der Begriffe „<i>Surface Web</i>“ (das indizierbare, über Suchmaschinen erreichbare Internet), dem „<i>Deep Web</i>“ (das nicht indizierbare Internet, beispielsweise Inhalte „hinter“ Login-Masken) und dem „<i>Dark Web</i>“ (Bereich des Internets, der nur über spezielle Software wie dem TOR-Browser erreicht werden kann), stellt Kaspersky einige Thesen zum Dark Web auf.</p> <p>Unter anderem werde das Dark Web irrtümlich als illegaler Cyber-Raum behandelt, obwohl es viele legitime Gründe für eine Nutzung des Dark Webs gibt, zum Beispiel in Ländern mit eingeschränkter Pressefreiheit. Auch biete es keine, wie oft geglaubt, vollständige Anonymität, sondern es existieren gewisse Möglichkeiten, Nutzer zu identifizieren. Kriminalbehörden ist es bereits mehrmals gelungen, Betreiber illegaler Marktplätze im Dark Web zu identifizieren und den Betrieb diese „<i>Hidden Services</i>“ einzustellen (<i>Silk Road, Alpha Bay</i>).</p>	
Bewertung:	Das Whitepaper behandelt es Thema Dark Web oberflächlich, technische Details sind nicht vorhanden. Die Inhalte bieten eine kurze Zusammenfassung des Sachstands zum Dark Web.	
Empfehlung:	Kenntnisnahme.	
Quellen:	./.	