Media Alert von SentinelOne vom 27.10.2020

SentinelOne warnt vor Zerologon

CVE-2020-1472, besser bekannt als Zerologon, ist eine kritische Schwachstelle in allen derzeit unterstützten Versionen von Microsoft Windows Server (Windows 2008 R2, 2012, 2016, 2019). Es handelt sich um eine Privilegien-Eskalations-Schwachstelle. Sie entsteht durch einen Fehler im Netlogon Remote Protocol (MS-NRPC). Die Sicherheitslücke ermöglicht es einem Angreifer, sich als ein System auszugeben, einschließlich des Maschinenkontos des Domain-Controllers selbst.

Inzwischen wurden weitere Möglichkeiten entdeckt, die Zerologon-Schwachstelle über das Zurücksetzen der Domain-Passwörter hinaus auszunutzen. Eine weitere Möglichkeit ist unter anderem die Extraktion von Domain-Passwörtern. Diese Entwicklung erhöht das Risiko, dem Unternehmen weltweit ausgesetzt sind. Damit ein solcher Angriff erfolgreich ist, müsste sich ein Angreifer zunächst Fernzugriff oder physischen Zugriff auf ein Gerät – wie z.B. einen Domänencontroller – im gleichen Netzwerk verschaffen. Gültige Domain-Zugangsdaten oder die Domain-Mitgliedschaft sind jedoch keine Voraussetzungen für einen erfolgreichen Angriff.

„Inzwischen warnen auch Hardware-Hersteller wie QNAP <https://www.qnap.com/en/security-advisory/qsa-20-07> oder öffentliche Stellen wie das BSI <https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/Zerologon_200924.html> vor der Ausnutzung der Schwachstelle. Unternehmen können sich nicht auf das Patchen allein verlassen und sollten stattdessen in moderne Sicherheitslösungen zur Erkennung von Angriffen investieren. Dank unserer Sicherheitsforscher gehörten wir zu den ersten, die den Angriff auf Endpoint-Ebene detektieren konnten. Leider sind solche Schwachstellen keine Seltenheit und es gibt nicht viel, was Unternehmen tun können, um sich darauf vorzubereiten. Deshalb ist es so wichtig auf KI-Sicherheitslösungen zu setzen," kommentiert Matthias Canisius, Regional Director CEU bei SentinelOne.

Seit der Bekanntgabe der Schwachstelle wurde Exploit-Code gefunden. Die CISA <https://www.borncity.com/blog/2020/09/21/cisa-warnung-patcht-eure-windows-server-gegen-cve-2020-1472-zerologon/> hat erklärt, dass die Schwachstelle ein inakzeptables Risiko darstelle und sofortige und dringende Maßnahmen erfordere. Obwohl Microsoft einen ersten Patch für Zerologon veröffentlicht hat, ist dies nur der Beginn einer schrittweisen Einführung, die der Hersteller des Betriebssystems voraussichtlich mindestens bis zum ersten Quartal 2021 dauern wird. In der Zwischenzeit weist Microsofts Hinweis darauf hin, dass das aktuelle Update nur unterstützte Windows-Geräte schützt, so dass ältere Windows-Versionen und andere Geräte, die mit Domänencontrollern über das Netlogon MS-NRPC-Protokoll kommunizieren, anfällig für Übergriffe sind.

Darüber hinaus verhindert der anfängliche Patch nicht einen Angriff, der Zerologon ausnutzt. Vielmehr fügt er eine Protokollierung hinzu, um unsichere RPC zu erkennen, und eine Registrierungseinstellung, um unsichere RPC zu deaktivieren, wenn es keine Geräte gibt, die das Protokoll verwenden. Die Herausforderung für die Sicherheitsteams von Unternehmen besteht darin, dass dies zu einem Bruch von Legacy-Anwendungen führen kann, wenn es einfach nur ausgeschaltet wird. Daher sind sie selbst mit dem derzeit verfügbaren Patch immer noch anfällig, wenn ihre Organisation die Registrierungseinstellung nicht deaktivieren kann.

Tipps zum Aufspüren und zur Abwehr von Zerologon-Missbrauch
Aus Endpunktsicht kann es schwierig sein, diesen Angriff zu erkennen, da sich der Angreifer im Wesentlichen auf eine Weise gegenüber der Domain authentifiziert, die dem Verhalten eines legitimen Benutzers/Kontos ähnelt. Darüber hinaus liegt der primäre Angriffsvektor auf der Netzwerkebene, im Gegensatz zur Interaktion mit dem Dateisystem eines Hosts. Infolgedessen ist die direkte Adressierung der Schwachstelle für viele traditionelle Endpunkt-Sicherheitslösungen „out-of-scope".

Weitere Informationen lesen Sie hier: https://www.sentinelone.com/blog/zerologon-cve-2020-1472-sentinelone-first-to-detect-on-the-endpoint/

Kontakt
Kafka Kommunikation GmbH & Co.
Auf der Eierwiese 1
82031 München-Grünwald

Dr. Bastian Hallbauer-Beutler
Lukas Reck
Kafka Kommunikation
089 74 74 70 580
sentinelone@kafka-kommunikation.de