



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Microsoft-Patchday im Februar: Vorherige Prüfung des DC-Updates erforderlich

CSW-Nr. 2021-189218-1031, Version 1.0, 08.02.2021

IT-Bedrohungslage*: 2 / Gelb

Sachverhalt

Im August 2020 warnte Microsoft erstmals vor der als „ZeroLogon“ bekannt gewordenen Schwachstelle im Netlogon-Remote-Protokoll (CVE-2020-1472) [MS20, BSI20]. Basierend auf dieser Sicherheitslücke können Angreifer per Netlogon eine Verbindung zum Domänencontroller (DC) herstellen und letztendlich das gesamte Netzwerk einer Organisation übernehmen.

Mit dem Patchday am Dienstag, den 9. Februar 2021, schließt der Hersteller diese Schwachstelle. Nach Installation des Updates auf allen Domänencontrollern wird bei Verbindungen zukünftig der Domain Controller Enforcement Mode als Standard verwendet [MS20A]. Dies hat zur Folge, dass nicht-konforme Verbindungen zum Domänencontroller blockiert werden und Geräte ein sicheres Remote-Protokoll (RPC) mit dem Netlogon-Kanal verwenden müssen.

Bewertung

Das BSI begrüßt die Veröffentlichung des Updates und somit die Schließung der o.g. Schwachstelle ausdrücklich. Mit einem CVSS-Score von 10 stellt ZeroLogon ein hohes Risiko für Organisationen und deren Netzwerke dar. Bei einer Nichtberücksichtigung der im Sachverhalt beschriebenen Auswirkungen des Patches kann es jedoch zu Verbindungsproblemen im Netzwerk kommen.

Maßnahmen

Das angekündigte Update sollte nach Erscheinen schnellstmöglich installiert werden. Dabei sind die folgenden Hinweise zu beachten:

- * 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Vor der Installation des Patches auf dem Domänencontroller sollte die Kompatibilität zunächst gemäß der gängigen BSI-Empfehlung zum Umgang mit Updates in einer Testumgebung geprüft werden [BSI20].

Weiterhin sollte sichergestellt werden, dass alle im Netzwerk befindlichen Geräte den Enforcement Mode unterstützen. Eine entsprechende Anleitung stellt Microsoft zur Verfügung. Laut [MS20C] kann der Enforcement Mode in besonderen Fällen auch per Gruppenrichtlinie umgangen werden. Dies gilt es aus Sicht des BSI jedoch zu vermeiden, um die Gefahr einer Kompromittierung des Netzwerks nachhaltig zu minimieren.

Links

[BSI20] Kritische Schwachstelle im Windows Netlogon Remote Protocol (ZEROLOGON)

https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2020/2020-244185-100_csw.html

[BSI20A] OPS.1.1.3: Patch- und Änderungsmanagement (Edition 2020)

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium Einzel PDFs/04 OPS Betrieb/OPS 1 1 3 Patch und Aenderungsmanagement Edition 2020.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/04_OPS_Betrieb/OPS_1_1_3_Patch_und_Aenderungsmanagement_Edition_2020.pdf)

[MS20] CVE-2020-1472 Netlogon Elevation of Privilege Vulnerability

<https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472>

[MS20A] Netlogon Domain Controller Enforcement Mode is enabled by default beginning with the February 9, 2021 Security Update

<https://msrc-blog.microsoft.com/2021/01/14/netlogon-domain-controller-enforcement-mode-is-enabled-by-default-beginning-with-the-february-9-2021-security-update-related-to-cve-2020-1472/>

[MS20B] How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472

<https://support.microsoft.com/en-us/topic/how-to-manage-the-changes-in-netlogon-secure-channel-connections-associated-with-cve-2020-1472-f7e8cc17-0309-1d6a-304e-5ba73cd1a11e>