Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Kritische Schwachstelle in Druckerspooler auf Microsoft Systemen

CSW-Nr. 2021-233732-1232, Version 1.2, 07.07.2021

IT-Bedrohungslage*: 3 / Orange

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:WHITE: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Im Rahmen des letzten Patchdays veröffentlichte Microsoft neben Sicherheitsupdates zusätzlich Informationen über die Schwachstelle CVE-2021-1675 [MS2021a]. Betroffen ist hier die Warteschlange (Spooler), die von Windows-Systemen zur Abarbeitung von Druckaufträgen genutzt wird. Von der Schwachstelle betroffen sind die Clientversionen Windows 7, Windows 8.1, Windows RT 8.1, Windows 10 (1607, 1809, 19009, 2004, 20H2, 21H1) als auch Serverversionen (2008, 2008 R2, 2012, 2012 R2, 2016, 2019, 2004, 20H2) von Microsoft Windows. Vom Hersteller wurde die Ausnutzung der Sicherheitslücke zunächst als aufwändig eingestuft. Die Schwachstelle ließ sich aus der Entfernung mit gültigen Anmeldeinformationen ausnutzen und erlaubt Codeausführung sowie die Eskalation von Privilegien.

In der Nacht vom 29.06. auf den 30.06.2021 wurde **Proof of Concept Exploitcode veröffentlicht** [GIT2021a, GIT2021a]. Die als *Printnightmare* benannten Exploits nehmen Bezug auf CVE-2021-1675 und nutzen eine **bislang ungepatchte Schwachstelle des Spooler-Dienstes** aus. Trotz des von Microsoft bereitgestellten Updates im Juni sind Angriffe auf den Spooler-Dienst weiterhin möglich. Dem BSI sowie weiteren Sicherheitsforschern ist das entfernte Ausführen des Exploits unter Verwendung von Anmeldeinformationen eines unprivilegierten Domänenbenutzers auf einem vollständig mit aktuellen

* 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.

Sicherheitsupdates versorgten Windows Server 2019 und Windows Server 2016 Domänencontroller gelungen. Der veröffentlichte Exploit-Code wurde bereits in Angriffswerkzeuge integriert [TR2021a, SA2021a].

Update 1:
Von Microsoft wurde ein Sicherheitshinweis veröffentlicht [MS2021c]. Die aktuelle Spooler-Schwachstelle wird darin unter CVE-2021-34527 geführt. Inwiefern jenseits von Domänencontrollern weitere Windows-Versionen konkret betroffen sind wird derzeit noch vom Hersteller untersucht. Der Sicherheitshinweis soll diesbezüglich fortlaufend aktualisiert werden.

Update 2:
Microsoft hat ein Out-of-Band Update für CVE-2021-34527 veröffentlicht. Dieses steht bislang für einige der betroffenen Windows-Versionen zur Verfügung. Für Windows 10 Version 1607, Server 2012 und 2016 sollen laut Microsoft in Kürze Sicherheitsupdates veröffentlicht werden. Außerdem wurden die Sicherheitshinweise aktualisiert [MS2021c].
Nach Einspielen des Updates können unprivilegierte Benutzer nur noch signierte Druckertreiber auf einem Druckserver hinzufügen. Soll auch dies nicht möglich sein, so stellt Microsoft in [MS2021d] einen Registry-Key "RestrictDriverInstallationToAdministrators" zur Verfügung. Wird der zugehörige Wert auf '1' gesetzt, so ist es unprivilegierten Benutzern in Folge auch nicht mehr möglich signierte Druckertreiber auf einem Druckserver hinzuzufügen.
Unsignierte und signierte Druckertreiber können dann nur noch mit administrativen Berechtigungen installiert werden.

Bewertung

Das BSI bewertet die Schwachstelle als kritisch. Da insbesondere auf Domänencontrollern der Spooler-Dienst ohne weitere Härtungsmaßnahmen standardmäßig aktiviert und authentisiert erreichbar ist, besteht hier ein besonderes Risiko. Mittels eines kompromittierten Arbeitsplatzrechners kann dadurch letztlich die Kontrolle über bspw. die Druckserver oder Domänencontroller im NT-Authorität\System Kontext und folglich potentiell das gesamte Netzwerk erlangt werden. Aufgrund dessen **ist von einer unmittelbaren Ausnutzung im Rahmen von Angriffen auszugehen**.

Maßnahmen

Da zur Mitigation aktuell nur der Spooler-Dienst deaktiviert werden kann, ist zu prüfen, ob der standardmäßig aktivierte Dienst zumindest auf Domänencontrollern abgeschaltet werden kann [MS2021b], [ITGSa], [ITGSb].

Durch die Deaktivierung kann auf diesen Systemen im Anschluss nicht mehr gedruckt werden. Weiterhin zu beachten ist dabei der unter [MS2021b] beschriebene Hinweis, dass durch eine Deaktivierung auf Domänencontrollern keine Druckbereinigung von veralteten Druckwarteschlangenobjekten aus dem Active Directory stattfindet. In Folge dessen müsste entweder eine manuelle Bereinigung oder eine Bereinigung mit Hilfe eines Automatisierungsskripts erfolgen.

Der Spooler-Dienst kann innerhalb einer Windowsdomäne über die Gruppenrichtlinien (Computer Configuration \Policies\Windows Settings\System Services\Print Spooler) und in lokal verwalteten Systemen über die Powershell oder die Diensteverwaltung (services.msc) deaktiviert werden.

Sobald in diesem Zusammenhang ein neues Update verfügbar ist, sollte dieses unmittelbar geprüft und eingespielt werden.

Update 1:
Neben der bereits beschriebenen Deaktivierung des Spooler-Dienstes (Option 1) wird im Sicherheitshinweis von Microsoft auch ein zweiter Workaround aufgeführt: "Disable inbound remote printing through Group Policy" (Option 2) [MS2021c]. Das Deaktivieren der GPO "Allow Print Spooler to accept client connections" führt laut Hersteller dazu, dass eingehende Druckaufträge aus dem Netzwerk verhindert werden. Ein lokales Drucken bleibt weiterhin möglich.

Dieser Workaround verhindert nur die Remotecodeausführung. Die Möglichkeit einer lokalen Codeausführung und Privilegieneskalation bleibt somit weiterhin bestehen.

Update 2:
Aufgrund der Kritikalität der vorliegenden Schwachstelle und der von Microsoft angegebenen Ausnutzung sollten die bereitgestellten Updates schnellstmöglich angewendet werden. Andernfalls sind die angegebenen Mitigationsmaßnahmen zu berücksichtigen.

Neben Einspielen des Patches sollte auch geprüft werden, ob der in [MS2021d] beschriebene Registry-Key mit dem Wert '1' gesetzt werden kann, um die Installation von unsignierten und signierten Druckertreibern auf dem Druckserver durch unprivilegierte Benutzer zu unterbinden.

Zusätzlich sollte geprüft werden, dass, wie in [MS2021c] beschrieben, die Point and Print Konfiguration gehärtet ist, so dass eine Warnung und eine Aufforderung zur Rechteerhöhung (Elevation Prompt) erscheinen.
Diese Standardkonfiguration sollte sicherheitshalber in der Registry bzw. den Gruppenrichtlinien überprüft werden und ggf. angepasst werden.
Die zugehörigen Registry-Keys unter HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printer\PointAndPrint sollten wie folgt gesetzt sein:

- **NoWarningNoElevationOnInstall = 0**
- **NoWarningNoElevationOnUpdate = 0**

Diese Registry-Einträge existieren nur, wenn die Group-Policy (Computer Configuration\Administrative Templates \Printers\Point and Print Restrictions) konfiguriert ist. Ansonsten liegt die Standardkonfiguration bereits vor.

Links

[GIT2021a] - PrintNightmare (CVE-2021-1675): Remote code execution in Windows Spooler Service
https://github.com/afwu/PrintNightmare

[GIT2021b] -CVE-2021-1675
https://github.com/cube0x0/CVE-2021-1675

[ITGSa] - BSI, IT-Grundschutz, Allgemeiner Server SYS.1.1.A6 - Deaktivierung nicht benötigter Dienste (B)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/07_SYS_IT_Systeme/SYS_1_1_Allgemeiner_Server_Edition_2021.pdf

[ITGSb] - BSI, IT-Grundschutz, Allgemeiner Client SYS.2.1.A16 - Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen (S)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/07_SYS_IT_Systeme/SYS_2_1_Allgemeiner_Client_Edition_2020.pdf

[MS2021a] Sicherheitsanfälligkeit im Windows-Druckerspooler bezüglich Remotecodeausführung
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1675

[MS2021b] Sicherheitsbewertung: Domänencontroller mit verfügbarem Druckspoolerdienst
https://docs.microsoft.com/de-de/defender-for-identity/cas-isp-print-spooler

[MS2021c] Windows Print Spooler Remote Code Execution Vulnerability
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

[MS2021d] KB5005010: Restricting installation of new printer drivers after applying the July 6, 2021 updates
https://support.microsoft.com/en-us/topic/kb5005010-restricting-installation-of-new-printer-drivers-after-applying-the-july-6-2021-updates-31b91c02-05bc-4ada-a7ea-183b129578a7

[SA2021a] PoC exploit for CVE-2021-1675 RCE started circulating online
https://securityaffairs.co/wordpress/119502/hacking/2021-1675-rce-poc.html

[TR2021a] PoC exploit accidentally leaks for dangerous Windows PrintNightmare bug
https://therecord.media/poc-released-for-dangerous-windows-printnightmare-bug/

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs) welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

   Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

2) Welche Einstufungen existieren?

   - **TLP:WHITE: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
     Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.