Microsoft Patchday Februar 2022

Riskante Schwachstellen im Windows-Kernel und DNS-Servern

09.02.2022 | Von Thomas Joos

Zum Patchday im Februrar 2022 veröffentlicht Microsoft knapp 50 Sicherheitsupdates für seine Produkte und zusätzlich noch 20 Patches für Microsoft Edge. Zwar gibt es in diesem Monat keine kritischen Updates, dafür aber viele als wichtig eingestufte Aktualisierungen.

Beim Februar-Patchday 2022 gibt es zwar keine kritischen Security Patches, aber einige Schwachstellen sollten Admins dennoch umgehend schließen.
(Logo: Microsoft)

Die Patch-Situation beim Microsoft-Patchday im Februar 2022 ist weniger dramatisch als sonst. Dennoch gibt es unter den vielen Updates auch zahlreiche als "wichtig" eingestufte Patches. Dafür fehlen im Februar kritische Updates. Keine der aktuellen Lücken sind bereits aktiv unter Angriff. Allerdings ist eine Lücke öffentlich bekannt.

Es ist daher davon auszugehen, dass hier in Zukunft auch Angriffe erfolgen werden. Das Schließen dieser Lücke ist daher sehr anzuraten. Es gibt aber noch mehr Lücken, die zwar nicht öffentlich bekannt sind und bereits ausgenutzt werden, die aber dennoch sehr schnell geschlossen werden sollten.

Öffentlich bekannte Schwachstelle im Windows-Kernel: Erhöhte Berechtigungen möglich

Die Schwachstelle CVE 2022-21989 <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21989> ist öffentlich bekannt und als „Wichtig“ eingestuft. Daher sollte das Update für diese

Lücke möglichst schnell geschlossen werden. Betroffen davon sind Arbeitsstationen mit Windows 10/11, aber auch Server bis hin zu Windows Server 2022. Durch das Ausnutzen dieser Lücke kann ein Angreifer sich erhöhte Rechte in Windows aneignen und dadurch auch Code und Malware mit Admin-Rechten ausführen.

Kritisch: Remoteausführung auf DNS-Servern in Active Directory möglich

Die Schwachstelle CVE-2022-21984 <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21984> ermöglicht Angreifern die Remoteausführung von Code. Auch wenn diese Lücke aktuell noch nicht öffentlich bekannt ist, sollte sie so schnell wie möglich geschlossen werden.

Die Schwachstelle betrifft die dynamischen Updates auf DNS <https://www.ip-insider.de/was-ist-dns-domain-name-system-a-579256/> -Servern, die vor allem in Active Directory <https://www.ip-insider.de/was-ist-ein-active-directory-a-626455/> zum Einsatz kommen. Da es sich dabei oft auch im die Domänencontroller <https://www.ip-insider.de/was-ist-ein-domaenencontroller-a-626094/> handelt, sollten Admins schnell reagieren und den Patch installieren. Durch die Lücke ist die komplette Übernahme des DNS-Servers möglich. Die Lücke ist nur deshalb nicht als kritisch eingestuft, weil dynamische Updates erst aktiviert werden sollten. In sehr vielen AD-Umgebungen ist das der Fall und macht hier die Lücke auch zur kritischen Lücke.

Remoteausführung auf Hyper-V-Hosts möglich – bis hin zu Windows Server 2022

Da auf Hyper-V <https://www.ip-insider.de/was-ist-hyper-v-a-868699/> -Hosts nicht nur ein Server betroffen ist, sondern alle VMs in dieser Umgebung, sollten Lücken auf diesen Servern schnell geschlossen werden. Die Lücke CVE 2022-21995 <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21995> ermöglicht ebenfalls die Remotecodeausführung, in dem eine VM <https://www.ip-insider.de/was-ist-eine-virtuelle-maschine-virtual-machine-a-941269/> übernommen wird. Von der Lücke sind alle aktuellen Windows-Versionen betroffen, bis hin zu Windows 10/11 und Windows Server 2019/2022. Auch Windows Server 2022 Datacenter: Azure Edition erhält hier ein Update.