

Security Alert: Zero-Day-Lücken in MS Exchange ermöglichen Industriespionage – Expertenkommentar von Tim Berghoff

Bochum (Deutschland), 03. März 2021

Microsoft hat gestern Abend Notfall-Patches für insgesamt vier bisher ungepatchte Sicherheitslücken in Microsoft Exchange veröffentlicht / Die Lücken werden derzeit von staatlichen Akteuren aktiv ausgenutzt.

Vier Zero-Day-Sicherheitslücken in lokal installierten Versionen von Microsoft Exchange ermöglichen sowohl eine Authentisierung ohne Nutzerdaten, das Schreiben und Ausführen von beliebigem Code als auch die Ausleitung von Unternehmensdaten. Angreifer könnten sogar ganze Offline-Adressbücher und Mailboxen exfiltrieren. Daher rät Microsoft, die bereitgestellten Updates unverzüglich zu installieren. Alle vier Zero-Day-Lücken haben eine CVE zugewiesen bekommen ([CVE-2021-26855](#), [CVE-2021-26857](#), [CVE-2021-26858](#) und [CVE-2021-27065](#)). Betroffen sind lokale Installationen von Microsoft Exchange. Die Online-Versionen von Exchange sind von den Lücken nach derzeitigen Erkenntnissen nicht betroffen.

G DATA CyberDefense AG
Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299



Es gebe eindeutige Anzeichen dafür, dass eine Gruppierung namens HAFNIUM die Lücken derzeit aktiv nutzt. Experten zur Folge operiert die Gruppe aus dem asiatischen Raum und im Auftrag einer Regierung.

„Auch wenn Unternehmen vermehrt Chatplattformen wie MS-Teams, Slack oder andere nutzen, sind Mailserver nach wie vor das Herzstück vieler Unternehmen. Hier liegen extrem viele unternehmenskritische Daten. Notfall-Patches von Microsoft bedeuten in der Regel vor allem eins: Überstunden für IT-Admins. Dass Angreifer die Sicherheitslücke bereits aktiv ausnutzen, zeigt, wie wichtig zeitnahes Handeln in diesem Fall ist“, sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense AG.

Einblick in Postfächer

Angreifer, die die Lücken ausnutzen, geben sich – vereinfacht gesagt – als Exchange-Server aus. Dadurch ist es möglich, die Zugänge zu kompromittieren, ohne selbst Kenntnis von Passwörtern zu haben. Damit ist ein direkter Einblick in das Postfach des jeweiligen Nutzers möglich. Schon diese Sicherheitslücke allein wäre hochgradig kritisch. Die übrigen Lücken werden unter anderem dafür genutzt, so genannten Webshells auf dem Server einzurichten. Über diese können Angreifer dann jederzeit von außen

Pressemitteilung

auf Informationen zugreifen. Es gilt als gesichert, dass die Gruppierung hinter HAFNIUM vor allem Forschungseinrichtungen (speziell solche, die in der Erforschung ansteckender Krankheiten aktiv sind), NGOs und Zulieferunternehmen für die Rüstungsindustrie ins Visier nimmt.

„APT-Gruppen wie Hafnium setzen in der Regel nicht auf kurzfristige und sichtbare Angriffe wie Ransomware – sondern versuchen über Zeit möglichst viele vertrauliche Daten zu sammeln. Fokus der Aktivitäten dürfte also in der Regel Industriespionage sein und nicht die klassische Verwertungskette organisierter Cybercrime-Gangs“, sagt Berghoff.

Verdächtige Zeichen

Da die Täter auch bereits ganze Postfächer in Form der lokal gespeicherten Archivdatei ausgeleitet haben, kann man die Kritikalität der entdeckten Sicherheitslücken nicht hoch genug bewerten. Es gibt jedoch eindeutige Anzeichen, anhand derer sich klar erkennen lässt, ob sich derzeit jemand mit Hilfe dieser Kombination aus Zero-Day-Lücken Zugriff auf Unternehmensdaten verschafft hat. Eines dieser Anzeichen ist recht typisch für die Ausleitung von Daten. Beispielsweise speichern die Täter Kopien der lokalen Outlook-Datei in einem ZIP-Archiv, welches in %ProgramData% abgelegt wird. Ein regelmäßiger Blick kann sich also an dieser Stelle lohnen. Typischerweise bereiten die Täter die Ausleitung von Daten vor, indem sie die erbeuteten Informationen an einer Stelle sammeln und von dort aus dann nach außen senden. Im Falle von HAFNIUM wurde ein öffentlicher Online-Filesharing-Dienst namens „Mega“ verwendet.

Ein ebenfalls oft beobachtetes Anzeichen für verdächtige Aktivitäten in diesem Zusammenhang: Prozess-Dumps, die in bestimmten Verzeichnissen wie c:\windows\temp abgelegt sind.

IoC-Liste

Auf der Microsoft-Webseite ist eine sehr ausführliche Auflistung von Merkmalen und Kenndaten zu finden, die auf eine Ausnutzung durch HAFNIUM hindeuten. Darunter befinden sich bestimmte Aktivitäten, die sich in Logdateien wiederfinden. Ein Beispiel dafür wäre das automatisierte Herunterladen zusätzlicher Werkzeuge aus einem öffentlichen Github-Repository.

Die vollständige Liste finden Sie [auf der Internetseite von Microsoft](#)



G DATA CyberDefense AG Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299