Landespolizeipräsidium · Mainzer Straße 134-146. ·66121 Saarbrücken

Landespolizeipräsidium
LPP 2 Kriminalitätsbekämpfung/ Landeskriminalamt

Dezernat LPP 222

Dienst-gebäude: **Hellwigstraße 8-10**
66121 Saarbrücken

Bearbeiter_in: Schmitt M.O.KHK
Tel.: 0681 962 – 2431
Fax: 0681 962 –2445
E-Mail: cybercrime@polizei.slpol.de

Az: 23/2022

Datum: 05.10.2022

Information des Dezernates Cybercrime
des Landespolizeipräsidiums Saarland

Warnmeldung hinsichtlich neuer Zero-Day-Lücke in Exchange

Seit Ende September 2022 ist eine weitere und bereits aktiv angegriffene Zero-Day-Lücke in Microsofts Exchange-Server bekannt. Potentielle Angreifer können trotz der Umsetzung bisher angebotener Workarounds, immer noch Server kompromittieren.

Die Angriffe kombinieren zwei Schwachstellen. Eine,

durch welche die Täter ihre Rechte ausweiten könnten
(CVE-2022-41040, CVSS 8.8, Risiko "hoch")

sowie eine weitere, welche

das Ausführen von beliebigem Code aus der Ferne ermöglicht
(CVE-2022-41082, CVSS 8.8, hoch).

Schwachstellen-Name: ProxyNotShell
CVE-2022-41082 ist ein Angriffsvektor, der auf Microsofts Exchange Server abzielt und Angriffe mit geringer Komplexität und geringen erforderlichen Privilegien ermöglicht.

Wenn die betroffenen Dienste verwundbar sind, kann ein authentifizierter Angreifer den zugrundeliegenden Exchange Server durch Ausnutzung der vorhandenen Exchange Power Shell kompromittieren, was zu einer vollständigen Kompromittierung führen kann.

Mit Hilfe von CVE-2022-41040, kann ein Angreifer CVE-2022-41082 aus der Ferne auslösen, um Befehle aus der Ferne auszuführen.

Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken

Beachten Sie:

Das Blockieren des eingehenden Datenverkehrs zu Exchange-Servern mit kritischen Asserts ist ebenfalls eine Option, allerdings nur dann praktikabel, wenn eine solche Maßnahme keine Auswirkungen auf lebenswichtige Abläufe hat und idealerweise als vorübergehende Maßnahme angesehen werden sollte, bis Microsoft einen verifizierten Patch herausgibt.

Die Polizei rät:

- Prüfen Sie anhand der bisher veröffentlichten Workarounds, ob Ihr System anfällig ist.
- Passen Sie nach Möglichkeit Ihr System anhand der Workarounds entsprechend an.
- Verfolgen Sie die weitere Berichterstattung hinsichtlich ProxyNotShell aufmerksam.
- Installieren Sie bei Bereitstellung eines verifizierten Patches diesen umgehend.

Quellen:

- https://www.heise.de/news/Exchange-Server-Zero-Day-Bisheriger-Workaround-unzureichend-7283072.html
- https://microsoft.github.io/CSS-Exchange/Security/EOMTv2/
- https://gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html
- https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/
- https://learn.microsoft.com/en-us/powershell/exchange/control-remote-powershell-access-to-exchange-servers?view=exchange-ps&viewFallbackFrom=exchange-ps%22%20%5Cl%20%22use-the-exchange-management-shell-to-enable-or-disable-remote-powershell-access-for-a-user

Mit freundlichen Grüßen,

i.A. KHK M.O. Schmitt

Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken