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: 4/2021

Datum: 08.03.2021

Information der
Zentralen Ansprechstelle Cybercrime (ZAC) des Landespolizeipräsidiums Saarland

Angriff auf Microsoft Exchange Server
- Prüf Skript für Administratoren

Derzeit kommt es zu gezielten Angriffen auf Microsoft Exchange Server 2010, 2013, 2016 und 2019. Mehrere Schwachstellen, welche die Angriffe ermöglichen, werden als „kritisch“ eingestuft.

Gelingt dies, ist ein Ausnutzen der Sicherheitslücken **(CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065)** möglich. Betreiber von Exchange Servern sollten umgehend alle aktuellen Sicherheitsupdates installieren. Microsoft Exchange Online ist nicht von den Lücken betroffen.

Für Exchange Server haben die Entwickler folgende abgesicherte Versionen veröffentlicht:

- Exchange Server 2010 (RU 31 for Service Pack 3)
- Exchange Server 2013 (CU 23)
- Exchange Server 2016 (CU 19, CU 18)
- Exchange Server 2019 (CU 8, CU 7)

Die Firma **Microsoft** hat jetzt ein **Prüf-Skript bereitgestellt**.
Mit diesem können Administratoren ihre Systeme prüfen.

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Mit dem auf Microsofts GitHub-Repository „CSS-Exchange“ bereitgestellten PowerShell-Skript (betrieben von den 'Support Engineers for Microsoft Exchange Server') steht ein PowerShell-Skript bereit, das einen oder mehrere Exchange-Server auf Spuren untersucht, die ein erfolgreicher Angriff hinterlässt.

Kombiniert ein Angreifer die Schwachstellen mit den Bezeichnungen CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 und CVE-2021-27065 miteinander, bezeichnet man diesen Angriff als "ProxyLogon". Er erlaubt das Ausführen von Code aus der Ferne und setzt aktivierten Outlook Web Access voraus (OWA).

Das Skript „Test-ProxyLogon.ps1“ bei GitHub sucht nach Angriffsmerkmalen, die für ProxyLogon typisch sind. Das Skript fasst die manuellen Tests zusammen und macht es Administratoren erheblich einfacher, ihre Exchange-Server zu prüfen. Es durchsucht Exchange-Logs, Exchange-HttpProxy-Logs und Windows-Application-Event-Logs.

Auf einem lokalen Exchange-Server (auf der Exchange Management Shell) gibt das Skript seine Ergebnisse direkt aus:

.|Test-ProxyLogon.ps1

Die Ausgabe lässt sich speichern:

.|Test-ProxyLogon.ps1 -OutPath $home|desktop|logs

Wer mehrere Exchange-Server betreibt, kann alle Systeme zugleich untersuchen (und das Ergebnis speichern):

Get-ExchangeServer | .|Test-ProxyLogon.ps1 -OutPath $home|desktop|logs

<u>Die Polizei rät</u>

- Prüfen Sie zeitnah ob Sie als Betreiber von Exchange Servern(n) betroffen sind.
- Spielen Sie SOFORT die mitgeteilten Updates ein.
- Kann eine Kompromittierung festgestellt werden, erstatten Sie bei der Ihnen nächst gelegenen Polizeidienststelle Anzeige.

Anbei wird die Warnmeldung des BSI mitübersandt.

<u>Zentrale Ansprechstelle Cybercrime (ZAC)</u>
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Polizei

SAARLAND

Quellen:

https://www.heise.de/news/Angriffe-auf-Exchange-Server-Microsoft-stellt-Pruef-Skript-fuer-Admins-bereit-5073827.html

https://github.com/microsoft/CSS-Exchange/tree/main/Security

https://www.bleepingcomputer.com/news/microsoft/this-new-microsoft-tool-checks-exchange-servers-for-proxylogon-hacks/

https://www.heise.de/news/Jetzt-patchen-Angreifer-attackieren-Microsoft-Exchange-Server-5070309.html

https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-197772-1132.pdf?__blob=publicationFile&v=8

Mit freundlichen Grüßen,

i.A.
KHK M.O. Schmitt
Zentrale Ansprechstelle
Cybercrime Saarland

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de

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

Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html