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: 32/2021

Datum: 08.09.2021

Information der
Zentralen Ansprechstelle Cybercrime (ZAC) des Landespolizeipräsidiums Saarland

Warnmeldung der zentralen Ansprechstelle Cybercrime (ZAC) Saarland hinsichtlich maliziöser Office-Dokumente

Derzeit wird durch Unbekannte Täter eine Sicherheitslücke in Windows genutzt.

Die Täter bringen gezielt präparierte Microsoft-Office-Dokumente in Umlauf, die nach dem Öffnen Windows-Computer mit Schadcode infizieren. Mit den Standardeinstellungen von Office sollten laut der Aussage von Microsoft zusätzliche Schutzmaßnahmen die aktuellen Angriffe verhindern. Administratoren können Systeme über einen Workaround absichern.

Laut der Warnmeldung von Microsoft zufolge, betrifft die mit dem Bedrohungsgrad "hoch" eingestufte Sicherheitslücke **(CVE-2021-40444)** die HTML-Rendering-Engine MSHTML von Windows. Diese setzt neben dem Internet Explorer auch Microsoft Office ein.
Von der Lücke sind **Windows 8.1 bis 10 und Windows Server 2008 bis 2019 betroffen**.

Ablauf des Angriffs
Öffnet das Opfer eine präparierte Office-Datei, so wird durch den Internet Explorer eine von Angreifern kontrollierte Website öffnet. Über ein darauf platziertes ActiveX-Steuerelement platziert sich dann ein Trojaner auf Computer.

Standardmäßig öffnet Office Dokumente aus dem Internet aber in einem abgesicherten Modus. Außerdem soll der Schutzmechnanismus von Office Application Guard Dokumente isolieren und so Microsoft zufolge Angriffe dieser Art verhindern.

Generell gilt, dass man keine Dateien aus unbekannten Quellen öffnen sollte.
Auch wenn ein E-Mail-Absender bekannt ist, sollte man sich rückversichern, ob dieser die Datei wirklich versendet hat. Außerdem sollte man nicht, ohne nachzudenken, auf Links in Mails klicken.

Zentrale Ansprechstelle Cybercrime (ZAC)
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

Die Polizei rät:

- Generell gilt, dass keine Dateien aus unbekannten Quellen geöffnet werden sollten.
- Auch wenn ein E-Mail-Absender bekannt ist, sollte man sich rückversichern, ob dieser die Datei wirklich versendet hat.
- Außerdem sollte man nicht, ohne nachzudenken, auf Links in Mails klicken.
- Im Falle der Betroffenheit >> Erstatten Sie Anzeige.
- Sobald das Sicherheitspatch von Microsoft verfügbar ist, sollte dieses installiert werden.

Maßnahmen

Absicherung der Systeme
Microsoft stellt ein Sicherheitsupdate für den kommenden Patchday in Aussicht. Bis dahin sollten Administratoren Systeme über einen Workaround absichern und ActiveX-Steurelemente im Internet Explorer deaktivieren.

Um das zu tun, sollten Administratoren eine Textdatei erzeugen, folgenden Inhalt hineinkopieren und die Datei mit der Endung .reg speichern.

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0]

"1001"=dword:00000003

"1004"=dword:00000003

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1]

"1001"=dword:00000003

"1004"=dword:00000003

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2]

Zentrale Ansprechstelle Cybercrime (ZAC)
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

"1001"=dword:00000003

"1004"=dword:00000003

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3]

"1001"=dword:00000003

"1004"=dword:00000003

Im Anschluss muss die Datei mit einem Doppelklick geöffnet werden, um die Einträge der Windows Registry hinzuzufügen. Danach ist ein Neustart nötig.

Quellen:

https://www.heise.de/-6185702
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444
https://twitter.com/HaifeiLi/status/1435320653503254534

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
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