2025-017 CERT-Hessen Warnmeldung

19.05.2025, 16:00 Uhr

Manipulierte Versionen des Passwort-Managers KeePass in Umlauf

Tags: KeePass

Sachverhalt:
Sicherheitsforscher von WithSecure haben mehrere trojanisierte Versionen des Passwort-Managers KeePass entdeckt, die zum Download bereitstanden. Hierfür haben die Täter den Quelltext verändert und mit validen, inzwischen zurückgezogenen Zertifikaten signiert. Verteilt wurde die maliziöse Software durch Werbeanzeigen (Malvertising). Eine Installation der manipulierten Versionen führte zu einer Infektion mit der Malware Cobalt Strike Beacons, die unter anderem gespeicherte Daten exfiltrierte.

Betroffene Produkte:
KeePass 2.56 und 2.57

Bewertung:
Hessen3C bewertet den Sachverhalt als kritisch, da eine erfolgreiche Infektion unter Umständen zur Exfiltration von sensiblen Daten führen kann.

Empfehlung von Maßnahmen

Hessen3C spricht die dringende Empfehlung aus, Software ausschließlich aus vertrauenswürdigen Quellen zu beziehen. Die im HessenPC bereitgestellten Versionen sind geprüft und sicher.
Sollten Sie keinen HessenPC nutzen oder aus anderen Quellen installiert haben, empfiehlt

Hessen3C, anhand der nachfolgenden IoC's zu prüfen, ob die installierte KeePass-Version ggfs. manipuliert wurde:

KeePass-2.56-Setup.exe:
0000cff6a3c7f7eebc0edc3d1e42e454ebb675e57d6fc1fd968952694b1b44b3

KeePass.exe:
b51dc9ca6f6029a799491bd9b8da18c9d9775116142cedabe958c8bcec96a0f0

ShInstUtil.exe:
0fc4397d28395974bba2823a1d2437b33793127b8f5020d995109207a830761b

KeePass-2.57-Setup.exe:
0e5199b978ae9816b04d093776b6699b660f502445d5850e88726c05e933e7d8

KeePass.exe:
f1c6d8e594f85cd2cb844a3e8a90509ea137a67d7ef3f1b68a7be17df6ccac74

ShInstUtil.exe:
0f6cfb62ed2f118c776a049b93e5d3e7b226f74e7b466c1cfed3c449ed23a42b

Weitere maliziöse Dateien:

KeePass Installers
- 0e5199b978ae9816b04d093776b6699b660f502445d5850e88726c05e933e7d8
- 83a13d14e1cbc25e46be87472de1956ac91727553bb3f019997467b2bab2658f
- 2c510f9ae4472342faafb7f2a1f278160f3581ead8ccd5b7ba7951863dcba2f5
- c6ed28cc576340b9f0e9324bef8c8c428bcd32c5234be73b885caa20549f332b

KeePass Executables
- f1c6d8e594f85cd2cb844a3e8a90509ea137a67d7ef3f1b68a7be17df6ccac74
- 128a68a714f2f6002f5e8e8cfe0bbae10cd2ffe63d30c8acc00255b9659ce121
- 9cb3de5d5cc804235bd12c00ed45ec9d6116cc2c7523986dddb4d8643d54f5e5
- a5e643c6cda31e0c7691dab58febe2efce0e98c33b19fe495b74b885de134a22

ShInstUtil Files
- 0f6cfb62ed2f118c776a049b93e5d3e7b226f74e7b466c1cfed3c449ed23a42b

• 42d391dd7bfa4ea348ec1cd2620ea6458b37682f2b303e4a266e3d11a689f8ab
• 3733b3be213ee4b959b70ff070b46e30b2785b14f1aecb74e0788dd00a1e1853

WinSCP & TreeSize Free – Nitrogen

• 2dd75a7f9948d794e95539b9a9ccc6a1488fb64dbe099fea401a13f98166d6ae
• 5b48bbf2364f78812ea411ef41fb8b693a3965df13596b303e12f69908784d03
• fa3eca4d53a1b7c4cfcd14f642ed5f8a8a864f56a8a47acbf5cf11a6c5d2afa2

Hessen3C empfiehlt, die Hash-Werte der installierten Version mit den vorgenannten Hash-Werten (aus Malware-Samples) zu vergleichen und bei Betroffenheit das System in geeigneter Weise zu bereinigen. Wir bitte Sie weiter, uns Betroffenheiten unverzüglich als Sicherheitsvorfall zu melden.

WithSecure stellt maliziöse Domains bereit, die für eine Log-Auswertung genutzt werden können:

Malicious URLs – Incident

• hxxps://lvshilc[.]com/KeePass-2.56-Setup.exe
• hxxps://keeppaswrd[.]com/download.php
• hxxps://arch-online[.]com/List/com2/9O29EO3IRSBB
• hxxps://aicmas[.]com/List/com2/9O29EO3IRSBB
• hxxps://aicmas[.]com/Apply/readme/VJICARU60DC?[REDACTED]=[REDACTED]

Malicious URLs – Other

• 1ba8d063-0[.]b-cdn[.]net [Cobalt Strike NitrogenCluster C2]
• roatanforareason[.]com/wp-content/plugins/fix/TreeSizeFreeSetup.zip [Nitrogen Downloader]

Malicious Domains – Incident

• KeePass-info[.]aenys[.]com
• keeppaswrd[.]com
• lvshilc[.]com
• arch-online[.]com
• aicmas[.]com

Hessen3C empfiehlt, die Zugänge zu den maliziösen Domänen zu sperren, die Logfiles auszuwerten und gegebenenfalls geeignete Maßnahmen einzuleiten.

Weitere Quellen

https://labs.withsecure.com/content/dam/labs/docs/W_Intel_Research_KeePass_Trojanised_Malware_Campaign.pdf

https://cyberpress.org/hackers-exploit-keepass-password-manager-to-distribute-malware/

Hessen3C

Kurzfassung: Bedeutung der Traffic Light Protocol-Einstufungen

TLP:CLEAR: Unbegrenzte Weitergabe
Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

TLP:GREEN: Organisationsübergreifende Weitergabe
Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der CybersecurityCommunity) angehören.

TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

> TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe
> Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

TLP:RED: Persönlich, nur für benannte Empfänger Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.

Eine ausführliche Erläuterung zum Traffic-Light-Protokoll finden Sie im Dokument „*CERT-Verpflichtung-TLP.pdf*“ unter http://www.cert.hessen.de

Kontaktdaten:

Hessen CyberCompetenceCenter (Hessen3C)

Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz
Friedrich-Ebert-Allee 12
65185 Wiesbaden

Telefon, Notrufhotline: **+49 (611) 353 9900**
Fax: +49 (611) 353 1919
E-Mail: **cert@hessen3c.hessen.de**
Website: **https://www.hessen3c.de**