HUP-Log4Shell-Newsticker Startseite

HUP-Infos zum Thema Log4Shell

Wenn das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Warnstufe Rot ausruft, ist Handeln angesagt: Die Sicherheitslücke durch Log4Shell macht derzeit Webdienste wie iCloud, Steam und Twitter anfällig für unerwünschte Zugriffe auf Rechner. Dementsprechend ist das Schließen der Sicherheitslücken im Zusammenhang mit Log4Shell selbstverständlich auch für unsere Programmierer, Entwickler und Sicherheitsexperten:innen ein wichtiges Thema.

Damit die HUP-Lösungen so sicher wie möglich sind, analysiert unser Team die Lage, um geeignete Maßnahmen ergreifen zu können.

Auf dieser Seite finden Sie die jeweils aktuellen Infos der HUP.

Log4J Version 1.x

In Log4J Version 1.x existieren 2 bekannte Sicherheitslücken:

- CVE-2021-4104 (JMSAppender)
- CVE-2019-17571 (Log4J-Socket-Server)

Beide Lücken sind für alle in Auslieferung befindlichen HUP Produkte nicht relevant, da die jeweils kompromittierbaren Komponenten (JMSAppender bzw. Socket-Server) manuell per Konfiguration serverseitig aktiviert werden müssen.

Da in keinem unserer Produkte diese optionalen Komponenten aktiv sind, sind somit auch die bekannten Lücken nicht offen.

CVE-2019-17571 erfordert zudem Zugriff auf gesonderte Ports des Servers, was idR. allein schon durch die Firewalls blockiert wird.
Da der der Funktionsumfang von Log4J 1.x ausreichend für unsere Anwendungsfälle ist, planen wir kurzfristig kein Update dieser Komponente.

Zweite Systemsichtung abgeschlossen
Alexander Kiszelya Beitrag am Dez 15, 2021
Liebe Kundinnen und Kunden,

die HUP-Techniker haben die zweite Systemsichtung abgeschlossen und die Tabelle aktualisiert.

Ihr HUP-Team

HUP-Systeme in Bezug auf Log4Shell-Sicherheitslücke in der Übersicht
Alexander Kiszelya Beitrag am Dez 13, 2021
Liebe Kundinnen und Kunden,

in der Tabelle auf dieser Seite: **Übersicht HUP-Systeme** finden Sie eine Auflistung der HUP-Systeme und Informationen zu unseren Aktivitäten **und Ihren Aufgaben**.

Wir halten Sie weiter auf dem Laufenden!

Ihr HUP-Team

Um was geht es? -> Nützliche Links

Darum ist Log4Shell so gefährlich:
Über den Programmschnipsel Log4Shell und die festgestellte Sicherheitslücke durchsuchen kriminelle Hacker das Internet automatisiert gesamthaft nach verwundbaren Systemen. Deren Ziel ist es, zum Beispiel Daten zu entwenden. „Die Log4j-Schwachstelle steckt in einer oft genutzten Bibliothek für die Java-Software. Sie ist zwar auf einige ältere Versionen der Bibliothek mit dem Namen Log4j beschränkt, allerdings hat niemand einen vollen Überblick darüber, wo überall die gefährdeten Versionen von Log4j genutzt werden", fasst die SPIEGEL-Redaktion zusammen. Da durch die Lücke unauffällige Hintertüren eingebaut werden können, können Angriffe zeitlich versetzt stattfinden.

Anbei einige nützliche Links aus den Medien und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zum Thema "Log4Shell".

https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/211211_log4Shell_WarnstufeRot.html

https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Schwachstelle_Log4j_211210.html

https://www.spiegel.de/netzwelt/web/bundesbehoerde-warnt-vor-schwachstelle-in-weit-verbreiteter-software-a-55bc413b-2e01-446c-8ee6-5fabfee3b0f2

Herzlich willkommen
Alexander Kiszelya Beitrag am Dez 13, 2021
Liebe Kundinnen und Kunden,

wir heißen Sie auf unserem HUP-internen Newsticker zur Log4Shell-Sicherheitslücke herzlich willkommen. Hier halten wir Sie über unsere Aktivitäten auf dem Laufenden.
Schauen Sie doch bitte regelmäßig vorbei.

Ihr HUP-Team

https://www.heise.de/news/Kritische-Zero-Day-Luecke-in-log4j-gefaehrdet-zahlreiche-Server-und-Apps-6291653.html

https://www.heise.de/ratgeber/Schutz-vor-schwerwiegender-Log4j-Luecke-was-jetzt-hilft-und-was-nicht-6292961.html

https://www.spiegel.de/netzwelt/web/log4j-schwachstelle-koennte-laut-bsi-millionenschaeden-zur-folge-haben-a-cb8b76e1-52d0-4af9-8f35-fd7de156538b

BSI auf Twitter

https://tinyurl.com/9txhxzsu