

Übersicht Systeme (Log4Shell)

Hier finden Sie eine Übersicht der HUP Systeme und Komponenten, sowie deren aktuellen Status im Bezug auf die Log4Shell Sicherheitslücke.

Weitere Informationen über Log4Shell finden Sie auf der Hauptseite: [HUP-Log4Shell-Newsticker Startseite](#)

System	Version	Status	Stand	Maßnahmen
advantage	alle	Nicht betroffen	13.12.2021	Keine notwendig
Anzeigen (Unique/VL)	alle	Nicht betroffen	13.12.2021	Keine notwendig
Blattplanung & Umbruch (Unique/VL)	alle	Nicht betroffen	13.12.2021	Keine notwendig
Comet FA	alle	Nicht betroffen	13.12.2021	Keine Massnahmen notwendig
Comet PA	alle	Nicht betroffen	14.12.2021	Keine Massnahmen notwendig
HASSO	alle	Nicht betroffen	13.12.2021	Keine Massnahmen notwendig
HUP Portal powered by native:media	alle	Nicht betroffen	13.12.2021	Keine notwendig
INXMAIL	alle	Nicht betroffen	13.12.2021	Keine Massnahmen notwendig
Logo Verwaltung / Logo Manager	alle	Nicht betroffen	13.12.2021	Keine Massnahmen notwendig
Paradise Classic (ohne Portal Solutions)	alle	Nicht betroffen	13.12.2021	Keine Massnahmen notwendig
Print Redaktion (Unique/VL)	alle	Nicht betroffen	13.12.2021	Keine Massnahmen notwendig
PS. Callcenter	alle	Nicht betroffen	14.12.2021	Keine Massnahmen notwendig
PS. Complaint	alle	Nicht betroffen	14.12.2021	Keine Massnahmen notwendig
PS.Content	alle	Im Auslieferungszustand und nicht betroffen	13.12.2021	Das sollten Sie dringend tun: - Sicher stellen, dass auf den Servern keine kompromittierte Log4J Version in anderen (durch den Kunden) eingespielten Applikationen eingesetzt wird. - Protokolle auf verdächtige Requests und Aktivitäten prüfen. (Erkennbar am Text: jndi:) Das haben wir bereits getan: Prophylaktisch wurde durch den HUP Support der Konfigurationsschalter 'log4j2.formatMsgNoLookups=true' in allen durch HUP betreuten Kundeninstallationen gesetzt, um sicher zu stellen, dass die kompromittierbare Funktion inaktiv ist und bleibt.
PS.Content #Portal	alle	Im Auslieferungszustand und nicht betroffen	13.12.2021	Das sollten Sie dringend tun: - Sicher stellen, dass auf den Servern keine kompromittierte Log4J Version in anderen (durch den Kunden) eingespielten Applikationen eingesetzt wird. - Protokolle auf verdächtige Requests und Aktivitäten prüfen. (Erkennbar am Text: jndi:) Das haben wir bereits getan: Prophylaktisch wurde durch den HUP Support der Konfigurationsschalter 'log4j2.formatMsgNoLookups=true' in allen durch HUP betreuten Kundeninstallationen gesetzt, um sicher zu stellen, dass die kompromittierbare Funktion inaktiv ist und bleibt.
PS.eWorxx	alle	Im Auslieferungszustand und nicht betroffen	13.12.2021	Das sollten Sie dringend tun: - Sicher stellen, dass auf den Servern keine kompromittierte Log4J Version in anderen (durch den Kunden) eingespielten Applikationen eingesetzt wird. - Protokolle auf verdächtige Requests und Aktivitäten prüfen. (Erkennbar am Text: jndi:) Das haben wir bereits getan: Prophylaktisch wurde durch den HUP Support der Konfigurationsschalter 'log4j2.formatMsgNoLookups=true' in allen durch HUP betreuten Kundeninstallationen gesetzt, um sicher zu stellen, dass die kompromittierbare Funktion inaktiv ist und bleibt.

PS.Holiday	alle	Nicht betroffen	14.12.2021	Keine Massnahmen notwendig
PS.Retail	alle	Nicht betroffen	14.12.2021	Keine Massnahmen notwendig
PSA	alle	behoben	14.12.2021	Patches erfolgt, keine weiteren Massnahmen notwendig.
vMAP	alle	Nicht betroffen	20.12.2021	Das sollten Sie dringend tun: Keine Massnahmen notwendig Das haben wir bereits getan: Seit dem 13.12.21 hatten Log4J 2.15 getestet und begonnen auszuliefern und sind aber noch im Verlauf in den Test der 2.16 gegangen, welche wir dann auch ausgeliefert haben. Aktuell läuft noch der Test auf der 2.17. Diese werden wir ab 21.12.21 ausliefern.
WebAbo	alle	Nicht betroffen	14.12.2021	Das sollten Sie dringend tun: - Sicher stellen, dass in den Application-Servern (Tomcat, JBoss) keine kompromittierte Log4J Versionen in anderen (durch den Kunden) eingespielten Archiven eingesetzt wird. - Protokolle auf verdächtige Requests und Aktivitäten prüfen.
WebAnzeigen	alle	Im Auslieferungszustand und nicht betroffen	13.12.2021	Keine Massnahmen notwendig
Zugferd	alle	Nicht betroffen	14.12.2021	Keine Massnahmen notwendig
JEDOX	alle	betroffen	23.12.2021	Jedox ist von der Sicherheitslücke in Apache Log4j2 (CVE-ID CVE-2021-44228) betroffen, durch die Remotecode ausgeführt werden kann. Die kritische Sicherheitslücke in der Open-Source-Logging-Software Apache Log4j 2 hat die Apache Software Foundation (ASF) dazu veranlasst, ein Notfall-Sicherheitsupdate herauszugeben. Das sollten Sie dringend tun: Wir empfehlen die neueste Jedox Version 2021.3 zu installieren, in der die Sicherheitslücke bereits geschlossen ist. Für frühere Versionen (ab 2020.4 oder höher) können Patches installiert werden. Für ältere Versionen steht kein Hotfix bereit – hier muss ein Update auf die neueste Version 2021.3 erfolgen. Wir setzen uns hierzu möglichst zeitnah mit Ihnen in Verbindung.
PSA	alle	behoben	24.12.2021	Das sollten Sie dringend tun: Keine Massnahmen notwendig Das haben wir bereits getan: Alle produktiven Systeme haben eine Erweiterung der Konfiguration erhalten und wurden neugestartet.
PS.Devlivery	alle	behoben	24.12.2021	Das sollten Sie dringend tun: Keine Massnahmen notwendig Das haben wir bereits getan: Alle produktiven Systeme haben eine Erweiterung der Konfiguration erhalten und wurden neugestartet.