Sicherheitswarnungen

Übersicht

Liste der Sicherheitswarnungen

Lfd-Nr	Datum	Inhalt / Zusammenfassung	betroffene Versionen => Status	Status	Stand
2021-12-001	12.12.2021	CVE-2021-44228 log4j Exploit	• ica-1.5.x => OK • ica-1.7.x => OK	=> OK => OK	

Details zu Sicherheitswarnungen

2021-12-001 - log4j Exploit

Hintergrund:

Eine Sicherheitslücke in der Java Bibliothek log4j kann dazu führen, dass ein Angreifer beliebigen Code ausführen kann. Der Fehler wird unter CVE-2021-44228 geführt und wird als höchst kritisch eingestuft.

Der Fehler ist in den log4j Versionen 2.0 bis 2.14.x vorhanden. Ein Patch für logj4 2.x wurde bereits veröffentlicht.

Alle ICA Versionen verwenden das Logging-System, das von der Java EE / Jakarta Umgebung bereit gestellt wird. Je nach Version stellt die Laufzeitumgebung auch das auf log4j basierende Logging bereit. Für die Versionen ab ICA-1-7.x wird in der Regel slf4j als Implementierung für das Logging verwendet. Auf den Umgebungen für ICA-1.5.x teilweise log4j in der Version 1.x.

Stand 12.12.2021 / 15:59

Für die letzten verfügbaren Versionen der ICA Anwendung (ica-1.5.23 und ica-1.7.24) ist nach aktuellem Stand **keine** Gefährdung erkennbar.

Zur Prüfung wurde ein Exploit-Server aufgebaut, sowie eine Testanwendung, die die log4j Version 2.14.0 verwendet. Beim Logging der "vulnerable Codesequenz" in der Testanwendung konnte die Ausführung des "Remote Codes", bzw. der Verbindungsaufbau zum Exploit-Server nachgewiesen werden.

Danach wurde geprüft, ob das Logging in den aktuellen ICA-Versionen der ""vulnerable Codesequenz" ebenfalls zu einem Verbindungsaufbau des Exploit-Servers führt. Dabei folgendes festgestellt:

a) es wurde keine Verbindung zum exploit-Server ausgeführt

b) die "vulnerable Codesequenz" wurde ohne ***Interpretation*** in das Log geschrieben

Zusammenfassung

Nach aktuellem Stand sind die ICA-Anwendungen nicht von der Sicherheitslücke (CVE-2021-44228) betroffen.

Es ist jedoch nicht ausgeschlossen, dass die Umgebung, in der die ICA-Anwendung verwendet, wird so angepasst wurde, dass die von CVE-2021-44228 betroffenen Bibliotheken nicht doch verwendet werden. Dies betrifft insbesondere den meist verwendeten WebServer (Apache / NgNix), aber auch die verwendete und ggf. angepasste Java EE / Jakarta Umgebung.

Es wird aus diesem Grund dringend empfohlen den Empfehlungen des BSI zu folgen.