Sicherheitswarnung

BSI-Cyber-Sicherheitswarnung Java-Bibliothek Log4j

Bei der Verwendung von vernetzten Geräte- und Anlagenkomponenten mit Softwareelementen die Sicherheitslücken enthalten (hier: Java-Bibliothek Log4j („Log4Shell“)) besteht die Möglichkeit einer Gefährdung der Benutzer durch nicht oder fehlerhaft funktionierende softwaregesteuerte Sicherheitseinrichtungen!

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

Arbeitssicherheit

Ein IT-Dienstleister für IT-Sicherheit hat die „Log4Shell“ Schwachstelle in der weit verbreiteten Log4j Protokollierungsbibliothek für Java-Anwendungen veröffentlicht. Diese Bibliothek kommt in vielen Java-Anwendungen für die Erstellung von Log-Dateien zum Einsatz. Somit können auch sicherheitsrelevante Systeme direkt oder durch die in ihnen verbauten Komponenten oder für ihren Betrieb verwendeten Zusatzprogramme betroffen sein (Steuerungscomputer, Bedienpanels, Virtualisierungssoftware usw.). Zahlreiche Hersteller haben daher bereits Sicherheitshinweise zu ihren Produkten veröffentlicht (z. B. Siemens, Schneider Electric, Rockwell Automation).

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Bedrohungslage als extrem kritisch eingestuft (höchste Kategorie 4/Rot).

[1] Beispiel für eine einfache „defekt“-Kennzeichnung

Maßnahmen:

- *Prüfen Sie ob Sie Geräte und Anlagen in Ihrem Bereich im Einsatz haben, die die Java-Protokollierungsbibliothek Log4j verwenden. Dies gilt sowohl für unveränderte gekaufte als auch für selbstgebaute Geräte und Anlagen.*
- *Nehmen Sie betroffene Geräte und Anlagen, die abgeschaltet werden können, unverzüglich außer Betrieb.*
- *Kennzeichnen Sie diese Geräte als „defekt“ oder „zu prüfen“ und sichern Sie sie gegen versehentliches Wiedereinschalten (z. B. Schloss am Hauptschalter, Stecker umkleben mit Klebeband; Stecker in Tüte stecken und zubinden – siehe Abbildung 1).*
- *Prüfen Sei bei betroffenen Geräten und Anlagen, die nicht abgeschaltet werden können, bei jeder Benutzung die sicherheitsrelevanten Funktionen auf ordnungsgemäßen Betrieb (z. B Druck-/Temperaturüberwachungen, Lichtschranken, Zuhaltungen von Schutzabdeckungen).*
- *Für die Prüfung von Sicherheitsfunktionen sind ggf. zusätzliche Schutzmaßnahmen erforderlich (z. B. Abtrennungen, Sicherheitsabstand, Hilfswerkzeuge).*
- *Veranlassen Sie die Prüfung und ggf. Aktualisierung der Software aller betroffenen Geräte und Anlagen entsprechend den Herstellerhinweisen.*

BSI-Cyber-Sicherheitswarnung
https://kurzelinks.de/BSICSW-Log4Shell

Hinweis:

Die BSI-Cyber-Sicherheitswarnung enthält Verlinkungen zu verschiedenen Hilfestellungen, Lösungen, „Workarounds“ und Softwareupdates unter anderem auch der oben genannten Hersteller. Andere Anbieter werden sicher ähnlich verfahren. Setzen Sie Sich hierzu mit dem jeweiligen Hersteller oder Lieferanten in Verbindung.

Fachinfo Kritische Sicherheitslücken an Maschinen und Anlagen des Instituts für Arbeitsschutz (IFA) der DGUV
https://kurzelinks.de/DGUVIFA-Log4Shell