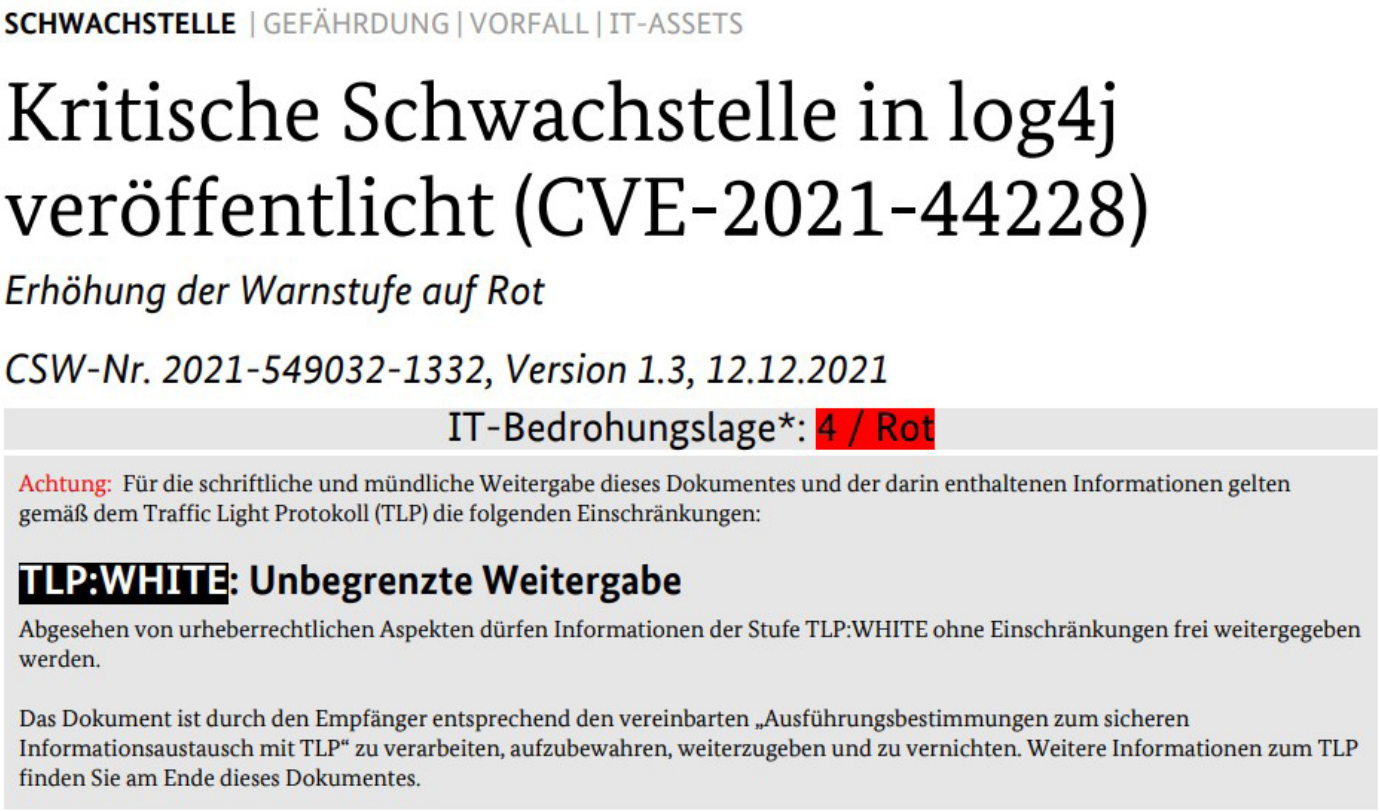
BSI – Warnstufe Rot:

Schwachstelle Log4Shell führt zu extrem kritischer Bedrohungslage

Die kritische Schwachstelle (Log4Shell) in der weit verbreiteten Java-Bibliothek Log4j führt nach Einschätzung des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu einer extrem kritischen Bedrohungslage. Das BSI hat daher seine bestehende Cyber-Sicherheitswarnung auf die Warnstufe Rot hochgestuft.

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Kritische Schwachstelle in log4j veröffentlicht (CVE-2021-44228)

Erhöhung der Warnstufe auf Rot

CSW-Nr. 2021-549032-1332, Version 1.3, 12.12.2021

IT-Bedrohungslage*: 4 / Rot

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:WHITE: Unbegrenzte Weitergabe

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

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Weitere Hintergründe zur „Kritischen Schwachstelle“ finden Sie hier als PDF. **Klicken Sie einfach auf das Bild und das PDF öffnet sich.**

Ursächlich für diese Einschätzung ist die sehr weite Verbreitung des betroffenen Produkts und die damit verbundenen Auswirkungen auf unzählige weitere Produkte. Die Schwachstelle ist zudem trivial ausnutzbar, ein Proof-of-Concept ist öffentlich verfügbar. Eine erfolgreiche Ausnutzung der Schwachstelle er-

möglicht eine vollständige Übernahme des betroffenen Systems. Dem BSI sind welt- und deutschlandweite Massen-Scans sowie versuchte Kompromittierungen bekannt. Auch erste erfolgreiche Kompromittierungen werden öffentlich gemeldet.

Das ganze Ausmaß der Bedrohungslage ist nach Einschätzung des BSI aktuell nicht abschließend feststellbar. Zwar gibt es für die betroffene Java-Bibliothek Log4j ein Sicherheits-Update, allerdings müssen alle Produkte, die Log4j verwenden, ebenfalls angepasst werden. Eine Java-Bibliothek ist ein Software-Modul, das zur Umsetzung einer bestimmten Funktionalität in weiteren Produkten verwendet wird. Es ist daher oftmals tief in der Architektur von Software-Produkten verankert. Welche Produkte verwundbar sind und für welche es bereits Updates gibt, ist derzeit nicht vollständig überschaubar und daher im Einzelfall zu prüfen. Es ist zu erwarten, dass in den nächsten Tagen weitere Produkte als verwundbar erkannt werden.

Das BSI empfiehlt insbesondere Unternehmen und Organisationen, die in der Cyber-Sicherheitswarnung skizzierten Abwehrmaßnahmen umzusetzen. Darüber hinaus sollten die Detektions- und Reaktionsfähigkeiten kurzfristig erhöht werden, um die eigenen Systeme angemessen überwachen zu können. Sobald Updates für einzelne Produkte verfügbar sind, sollten diese eingespielt werden. Darüber hinaus sollten alle Systeme auf eine Kompromittierung untersucht werden, die verwundbar waren.

Bundesamt für Sicherheit in der Informationstechnik
BSI - Bundesamt für Sicherheit in der Informationstechnik