Building a better working world

EY Cybersecurity Health Check

Schutz vor der kritischen Log4j-Schwachstelle (Log4Shell)

Lagebeschreibung

Eine neue ausnutzbare Sicherheitslücke, auch bekannt als CVE-2021-44228[1], wurde in der weitverbreiteten Apache Log4j 2 Java-basierten Protokollierungsbibliothek entdeckt, welche von der Apache Foundation entwickelt wurde und von einer Vielzahl von Enterprise Anwendungen und Cloud Services genutzt wird[2].

Bezeichnet als Log4Shell, wurde der Fehler als unauthentifizierte Remotecodeausführungs-Schwachstelle klassifiziert, welche mit simplen Angriffsmechanismen die komplette Systemübernahme auf Systemen mit den Log4j Versionen 2.14.1 oder älter ermöglichen.

Zahlreiche Apache Frameworks Standardkonfigurationen sind von dieser Schwachstelle betroffen, einschließlich Apache Struts2, Apache Solr, Apache Druid, Apache Flink, und andere.

Angreifergruppen scannen bereits aktiv das Internet nach verwundbaren IT-Systemen, welche anfällig für diese kritische und leicht ausnutzbare Schwachstelle sind und keine Authentifizierung der Angreifer erfordert[3]. BBC schreibt dazu: „Die Leichtigkeit, mit der Hacker die Schwachstelle ausnutzen können, ist ähnlich wie jemand, der herausfindet, dass er durch das Versenden eines Briefes mit einer bestimmten Adresse an ihr Postfach alle Türen in Ihrem Haus öffnen kann“[4]. Es besteht daher eine hohe Wahrscheinlichkeit, dass Angreifer schon jetzt oder in wenigen Wochen Hintertüren in infiltrierten System installieren, um weiteren Schadcode nachzuladen und sich im Netzwerk ihrer Opfer unbemerkt auszubreiten.

1 https://nvd.nist.gov/vuln/detail/CVE-2021-44228
2 https://logging.apache.org/log4j/2.x/index.html
3 https://www.cisa.gov/known-exploited-vulnerabilities-catalog
4 https://www.bbc.com/news/technology-59638308

Schiebt Ihre IT deswegen gerade Überstunden?

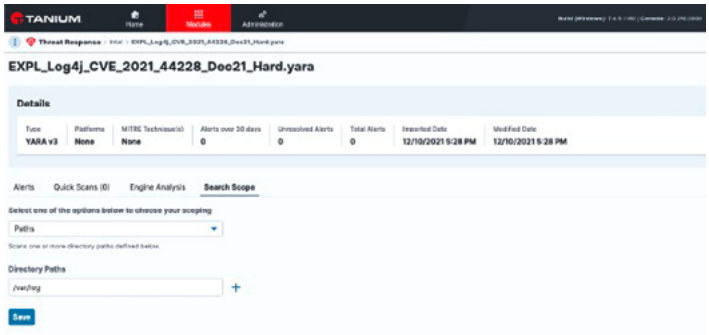
Die Sicherheitsbedrohung durch Schwachstellen in Programmbibliotheken von Middleware und Drittherstellern kann nur durch konsequentes **Schwachstellenmanagement auf Endpoint-Ebene** wirksam begegnet werden. Fehlt ein **technischer Schwachstellenscanner** in der Organisation, ist eine der wichtigsten **IT-Basishygienemaßnahmen** nicht umgesetzt. Aber selbst ein zentralisierter Schwachstellenscan kann tief verankerte Schwachstellen in Programmbibliotheken nicht identifizieren. Der einzig wirksame Schutz ist hier der Einsatz einer **agentenbasierten Endpoint Management und Security Lösung,** welche genaue Daten über den Status eines Endpoints wiedergibt, regelmäßig und automatisiert u. a. nach Schwachstellen sucht und diese durch Sicherheitsupdates oder das Setzen von Konfigurationsparametern innerhalb der Programmbibliotheken schnell beheben kann. Begleitend sollten **Vulnerability Disclosure Response Pläne** entwickelt werden, um die organisatorischen Prozesse auf das Schwachstellenmanagement abzustimmen und auf neue Bedrohungslagen vorbereitet zu sein.

Die aktuelle **Überlastung der IT-Abteilungen** durch Ermittlung der Ausbreitung und Auswirkung der Schwachstelle, sowie deren Behebung und der damit verbundenen **Kosten** sind ein deutliches Anzeichen, dass die **Cybersicherheit und das IT-Betriebsmanagement Ihrer Organisation noch Defizite** hat. Die Lizenz- und Betriebskosten einer Endpoint Management und Security Lösung hätten sich vermutlich bereits durch die aktuelle Bedrohungslage amortisiert. Finanzielle **Folge- und Reputationsschäden** aufgrund von erfolgreicher Ausnutzung der Schwachstelle und Datendiebstahl, sowie Datenzerstörung sind ebenfalls zu berücksichtigen.

Zeit zu handeln!

Organisationen mit Endpoint Management & Security-Lösung: Mitigieren oder patchen

Mit Hilfe ihrer Endpoint-basierten Lösung und Threat Hunting Methoden müssen Organisationen **verwundbare Log4j2 Instanzen und Anzeichen von entsprechenden Angriffsversuchen über alle Endpoints identifizieren. Upgrades** auf Log4j2-Version 2.16.0+ sollten vollständig ausgerollt werden.



Beispielhafter Screenshot aus einer Solution unseres Partners Tanium

Endpoints, welche Anzeichen einer Kompromittierung aufweisen, sollten **isoliert** werden. Alternativ können Schwachstellen auf Instanzen, welche nicht aktualisiert werden können oder dürfen, mit Hilfe der **Aktivierung von Dlog4j2.formatMsgNoLookups Systemeinstellungen** behoben werden. Für Log4j2-Versionen älter als 2.10 muss die JndiLookup class aus dem classpath entfernt werden.

Organisationen ohne Endpoint Management & Security Lösung

Der **EY Cybersecurity Health Check** mit unserer agentenbasierten **Partnerlösung von Tanium findet zügig verwundbare Instanzen,** inklusive Instanzen, die Log4j-Bibliotheken innerhalb von Software von Drittanbietern nutzen (Suche nach Log4j-Bibliotheken in JAR, EAR oder WAR Dateien). Die **Identifizierung von Anzeichen eines erfolgten Angriffs,** die Auswertung von Webserver-Logfiles, Isolierung kompromittierter Endpoints, **Ausrollen von Upgrades** oder die Konfiguration von Log4j2-Systemkonfigurationswerten wird automatisiert ermöglicht[5].

5 https://community.tanium.com/s/article/How-Tanium-Can-Help-with-CVE-2021-44228-Log4Shell

Cybersicherheits-Communities schlagen zusätzliche Maßnahmen zur Bereinigung vor, bis zuverlässige Upgrades zu Verfügung stehen. Sie können unsere EY Lösung einsetzen, um viele dieser Vorschläge organisationsweit zu implementieren und Konfigurationsparameter in Log4j-Bibliotheken zu setzen.

In Bereichen, in denen eine Endpoint Management & Security Lösung nicht in Frage kommt, müssen spezifischere Ansätze gefunden werden. Unsere Cybersecurity-Teams stehen Ihnen zur Seite, um weitere passende Maßnahmen für Ihr Unternehmen zu identifizieren und zu implementieren.

Abwehr digitaler Attacken durch EY

Nicht immer können Angriffe zeitnah bewälltigt werden. Deshalb bietet **„Cyber Incident Response"** bei EY umfangreiche und schnelle Unterstützung bei akuten Cyber-Sicherheitsvorfällen. Dank einer 24/7-Incident-Response-Hotline sind wir für unsere Mandanten rund um die Uhr erreichbar und unterstützen sie sofort bei der Krisenbewältigung. Kunden mit bereits bestehendem Rahmenvertrag können wir innerhalb von zwölf Stunden vor Ort und bereits zuvor remote unterstützen.

Unsere Cybersecurity-Leistungen auf einen Blick

- Technische automatisierte Identifizierung von Schwachstellen und IT-Härtungsmängeln
- Reifegradbestimmung der Cybersicherheit
- Ad-hoc-Reaktion auf Cyber-Sicherheitsvorfälle
- Cyber Threat Hunting
- Entwicklung von IoC & Signaturen für EDR, NSM, etc.
- Dashboarderstellung and SIEM-Regelsets
- Durchführung gerichtsfester Datensicherungen nach digitalforensischen Standards
- Bearbeitung konkreter IT-Sicherheitsvorfälle
- Kooperation mit Strafverfolgungsbehörden
- Unterstützung von Kunden vor Ort bei Identifikation und Bewertung möglicher IT-Sicherheitsvorfälle
- Aufbau effektiver Schutzmechanismen gegen Cyber-Sicherheitsvorfälle
- Fortgeschrittene Analyse forensischer Daten
- Netzwerkanalyse und die damit einhergehende Erkennung von Sicherheitsvorfällen
- Analyseberichte und gerichtsfeste Gutachten
- Databreach Report Support

Kontakt

Matthias Bandemer
Cybersecurity Leader Germany
+49 160 939 11976
matthias.bandemer@de.ey.com

Roland Ehlies
Cybersecurity
+49 160 939 20521
roland.ehlies@de.ey.com

Notfall-Hilfe

Thomas Koch
Digital Forensics / Incident Response
+49 160 939 17324
thomas.s.koch@de.ey.com

EY | Building a better working world

Mit unserer Arbeit setzen wir uns für eine besser funktionierende Welt ein. Wir helfen unseren Kunden, Mitarbeitenden und der Gesellschaft, langfristige Werte zu schaffen und das Vertrauen in die Kapitalmärkte zu stärken.

In mehr als 150 Ländern unterstützen wir unsere Kunden, verantwortungsvoll zu wachsen und den digitalen Wandel zu gestalten. Dabei setzen wir auf Diversität im Team sowie Daten und modernste Technologien in unseren Dienstleistungen.

Ob Assurance, Tax & Law, Strategy and Transactions oder Consulting: Unsere Teams stellen bessere Fragen, um neue und bessere Antworten auf die komplexen Herausforderungen unserer Zeit geben zu können.

Creative Design Germany | BKL 2112-039
ED None

ey.com/de