– Presseinformation der Controlware GmbH –

Controlware prüft Kundensysteme auf Log4J-Vulnerability

Dietzenbach, 14. Dezember 2021 – Die vor wenigen Tagen entdeckte Schwachstelle Log4Shell gehört zu den gefährlichsten der letzten Jahre. Die Security-Experten von Controlware helfen Kunden jetzt mit speziellen Schwachstellen-Scans und Compromise Assessments dabei, potenziell verwundbare Perimeter-Systeme zu lokalisieren und auf einen möglichen Schadsoftware-Befall hin zu untersuchen.

Am 9. Dezember 2021 dokumentierten Security-Experten erstmals eine gefährliche neue Schwachstelle: Die kritische Zero-Day-Vulnerability Log4Shell (CVE-2021-44228) in der beliebten Java-Logging-Library Log4J ermöglicht es Angreifern, durch das Logging eigener Payloads unerwünschten Programmcode auszuführen und die betroffenen Server auf diese Weise zu kompromittieren.

„Das Risikopotenzial dieser Schwachstelle ist enorm. Als Standardtool kommt Log4J im Business-Umfeld in unzähligen Java-Anwendungen zum Einsatz – und all diese Systeme können bei einer Remote Code Execution kompromittiert werden“, warnt Benjamin Heyder, Teamlead Cyber Defense Consulting bei Controlware. „Unternehmen sollten daher zeitnah prüfen, ob und in welcher Version die betroffene Logging-Library bei ihnen eingesetzt wird. Wenn ja, müssen sie diese sofort auf den neuesten Stand bringen – und dann im Rahmen eines Compromise Assessments prüfen, ob die Schwachstelle womöglich sogar schon für einen Angriff missbraucht wurde.“

Die neue Schwachstelle erhielt sofort nach Bekanntwerden eine CVSS-Bewertung (Common Vulnerability Scoring System) mit dem höchsten Risikograd 10,0. Das GitHub-Advisory, auf dem sie publiziert wurde, bescheinigt ebenfalls einen kritischen Schweregrad, und auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) vergab die Warnstufe Rot („Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrechterhalten werden.“). Nach aktuellen Berichten des BSI wurden zudem bereits die ersten Proofs-of-Concept eines Exploits auf GitHub und Twitter veröffentlicht. Diverse CERT-Einrichtungen – unter anderem das renommierte CERT New Zealand – berichten, dass inzwischen hunderte von Hosts das Internet

Sitz: Controlware GmbH Kommunikationssysteme ▪ Waldstraße 92 ▪ 63128 Dietzenbach ▪ GERMANY
Tel. +49 6074 858-00 ▪ Fax +49 6074 858-108 ▪ info@controlware.de ▪ www.controlware.de
Registergericht Offenbach a.M. ▪ HRB Nr. 6431 ▪ USt-IdNr. DE 113 539 225 ▪ Steuernummer 3523035235
Geschäftsführer: Bernd Schwefing, Michael Küchen

gezielt nach angreifbaren Servern scannen, und vermeldeten einen ersten erfolgreich eingesetzten Exploit mit einem Kryptominer. Das BSI berichtet auch bereits von Cobalt Strike Beacons, die über diesen Weg verteilt werden.

Schwachstellen-Scans und Compromise Assessments

Unternehmen, die ihre Perimeter-Systeme kostenlos scannen lassen möchten, um zu überprüfen, ob sie für den Exploit anfällig sind, steht das Controlware Team über das Kontaktformular jederzeit zur Verfügung. Ergänzend dazu bietet der Dietzenbacher IT-Dienstleister individuelle EDR Compromise Assessments, bei denen die Perimeter-Systeme auf einen möglichen Schadsoftware-Befall untersucht werden.

Über Controlware GmbH

Die Controlware GmbH, Dietzenbach, ist mit mehr als 800 Mitarbeitern und einem Umsatz von ca. 330 Mio. Euro einer der führenden unabhängigen Systemintegratoren und Managed Service Provider in Deutschland. Das 1980 gegründete Unternehmen entwickelt, implementiert und betreibt anspruchsvolle IT-Lösungen für die Data Center-, Enterprise- und Campus-Umgebungen seiner Kunden. Das Portfolio erstreckt sich von der Beratung und Planung über Installation und Wartung bis hin zu Management, Überwachung und Betrieb von Kundeninfrastrukturen durch das firmeneigene ISO 27001-zertifizierte Customer Service Center. Zentrale Geschäftsfelder der Controlware sind die Bereiche Network Solutions, Collaboration, Information Security, Application Delivery, Data Center & Cloud sowie IT-Management. Controlware arbeitet eng mit national und international führenden Herstellern zusammen und verfügt bei den meisten dieser Partner über den höchsten Zertifizierungsgrad. Das starke Unternehmen unterhält ein flächendeckendes Vertriebs- und Servicenetz mit 16 Standorten in DACH. Im Bereich der Nachwuchsförderung kooperiert Controlware mit renommierten deutschen Hochschulen und betreut durchgehend um die 50 Auszubildende und Studenten. Zu den Unternehmen der Controlware Gruppe zählen die Controlware GmbH, die ExperTeach GmbH, die Networkers AG und die productware GmbH.

Pressekontakt:
Stefanie Zender

Sitz: Controlware GmbH Kommunikationssysteme ▪ Waldstraße 92 ▪ 63128 Dietzenbach ▪ GERMANY
Tel. +49 6074 858-00 ▪ Fax +49 6074 858-108 ▪ info@controlware.de ▪ www.controlware.de
Registergericht Offenbach a.M. ▪ HRB Nr. 6431 ▪ USt-IdNr. DE 113 539 225 ▪ Steuernummer 3523035235
Geschäftsführer: Bernd Schwefing, Michael Küchen

Controlware GmbH
Tel.: +49 6074 858-246
Fax: +49 6074 858-220
E-Mail: stefanie.zender@controlware.de
www.controlware.de (Homepage)

Juliane Heermeier
fischerAppelt, relations GmbH
Tel.: +49 89 74 74 66 338
E-Mail: controlware@fischerappelt.de