ondeso | SUCCESS STORY

CVE-2021-44228: LOG4SHELL-PATCHING MIT ONDESO SR

Ein Cyber Security Engineer aus der Automobilindustrie stand vor der Herausforderung, die schwerwiegende Log4Shell-Schwachstelle auf 2.000 OT-Clients möglichst zeitnah zu schließen. Dank unserer bewährten Software ondeso SR fand er eine automatisierte Lösung zur schnellen Identifizierung und Behebung der Schwachstelle.

Die Log4Shell-Schwachstelle, auch unter CVE-2021-44228 bekannt, stellte ein ernstes Risiko für Unternehmen dar, da das weit verbreitete Apache Log4j-Softwareframework in zahlreichen Systemen und Anwendungen genutzt wird. Diese kritische Sicherheitsanfälligkeit ermöglichte es Angreifern, beliebigen Code auszuführen und Systeme zu kompromittieren, was zu erheblichen Sicherheitsrisiken führte. Ein Cyber Security Engineer, der für 2.000 OT-Clients in einem Produktionsunternehmen in der Automobilindustrie verantwortlich ist, erkannte die Dringlichkeit der Situation. Die Schwachstelle stellte eine ernsthafte Bedrohung für den laufenden Betrieb dar und erforderte eine schnelle Reaktion, um mögliche Produktionsausfälle und Sicherheitslecks zu verhindern. Da ondeso SR seit einigen Jahren weltweit im Konzern eingesetzt wird, entschied sich der Ingenieur, sowohl die Schwachstellen-Scans als auch die Behebung der Sicherheitslücke mit unserer Software durchzuführen. Sein Ziel war es, die Prozesse zu automatisieren, um die Schwachstelle schnell und zuverlässig zu beheben, ohne den Produktionsbetrieb zu unterbrechen.

LOG4SHELL: PATCHEN OHNE NEUSTART

Zur Behebung der Log4Shell-Schwachstelle entwickelten der Ingenieur und das Professional-Services-Team von ondeso zwei Operations, sprich automatisierte Arbeitsabläufe. Zuerst wurde ermittelt, welche der 2.000 OT-Clients betroffen waren. ondeso SR scannte gezielt nach Schwachstellenmerkmalen und dokumentierte betroffene Clients und Archive in der ondeso-Datenbank. Von den 2.000 Clients waren etwa 150 betroffen.

Die folgende Operation umfasste mehrere Schritte: Zunächst wurde eine Datensicherung der betroffenen Applikationen erstellt und bei Bedarf wurden Schreibschutzfilter oder Sicherheitskonfigurationen vorübergehend deaktiviert. Der Patch wurde von einer Netzwerkfreigabe kopiert und installiert. Dank interner Variablen in ondeso SR konnte der Verbindungsaufbau generisch definiert und client-spezifisch interpretiert werden. Dies ermöglichte eine flexible Handhabung, ohne die gesamte Operation ändern zu müssen, was die anfängliche Erstellung beschleunigte und die zukünftige Wartung vereinfacht. Die Installationsressourcen wurden anschließend bereinigt und die Ergebnisse in der Datenbank aktualisiert. Der Patch erfolgte ohne Neustart der Maschinen, sodass der laufende Betrieb nicht unterbrochen wurde. Einige OT-Clients wurden sofort gepatcht, während für andere ein geeignetes Wartungsfenster festgelegt wurde.

AUF EINEN BLICK

BRANCHE
Automobilindustrie

ANFORDERUNG
Schnelle und automatisierte Behebung der Log4Shell-Schwachstelle (CVE-2021-44228) auf produktionskritischen OT-Clients

LÖSUNG
Automatisierte Schwachstellen-Scans und Patch-Management durch ondeso SR

100 %
AUTOMATISIERTE ABARBEITUNG

AUSSAGEKRÄFTIGE REPORTS PER KNOPFDRUCK

SCHWACHSTELLEN INNERHALB VON 15 MIN. SCHLIESSEN

PATCHEN IN REKORDZEIT

Durch den Einsatz von ondeso SR konnte die Log4Shell-Schwachstelle in Windeseile geschlossen werden.
Andreas Decker, OT-Consultant bei ondeso, sagt: „Nachdem die Operation erfolgreich getestet wurde, konnten wir die Schwachstelle innerhalb von 15 Minuten beheben. Auch andere Werke können diese Operation nun einsetzen."
Mit ondeso SR war der Cyber Security Engineer somit in der Lage, die Schwachstelle effizient zu beheben, denn die automatisierte Lösung sparte ihm erheblich Zeit und reduzierte potenzielle Fehlerquellen. Zudem lieferten die umfassenden Reports einen klaren Überblick über den Fortschritt und die Ergebnisse des Patch-Prozesses.

Andreas Decker
OT-Consultant bei ondeso

„Nachdem die Operation erfolgreich getestet wurde, konnten wir die Schwachstelle innerhalb von 15 Minuten beheben."

---

ondeso

ondeso entwickelt Softwareprodukte speziell im Umfeld von Operational Technology sowie Industrie 4.0 und unterstützt bei der Automatisierung des OT-Client-Managements in der Produktion. Sowohl Anlagenbetreiber als auch Maschinen- und Anlagenbauer vertrauen seit Jahren auf ondeso-Produkte, welche branchenneutral und über die gesamte Breite der Produktionssysteme und -verfahren hinweg einsetzbar sind. Ob Leitsystem, HMI oder Steuerung – ondeso managt den Lifecycle von Industrie-PCs und bietet passgenaue Produkte auf höchstem technologischen und konzeptionellen Niveau – 100% made in Germany.

Möchten auch Sie das Client-Management Ihrer Industrie-PCs effizienter gestalten?

Kontaktieren Sie uns jetzt und vereinbaren Sie eine kostenlose Softwaredemo, um sich selbst ein Bild von ondeso SR zu machen.

Website: www.ondeso.com/kontakt
E-Mail: contact@ondeso.com
Telefon: +49 941 462932-0