Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Spring4Shell-Schwachstelle in Zutrittskontrollsystemen von Siemens

Nr. 2022-215640-1100, Version 1.1, 29.04.2022

IT-Bedrohungslage*: 2 / Gelb

Sachverhalt

Die Produkte Siveillance Identity, SiPass integrated und Operation Scheduler der Firma Siemens sind von der Spring4Shell-Schwachstelle (CVE-2022-22965) betroffen [SIE2022]. Bei den verwundbaren Produkten handelt es sich um Software, die vor allem im Bereich der physischen Sicherheit und Zutrittskontrolle eingesetzt wird.

Die Schwachstelle erlaubt einem entfernten, nicht authentifizierten Angreifer, beliebigem Code auf dem Zielsystem mit den Berechtigungen der Applikation auszuführen. Bekannte Exploits erfordern, dass die Applikation als WAR-Datei auf einem Tomcat läuft sowie dass JDK 9 oder höher zum Einsatz kommt. Konfigurationen, bei denen eine Spring Boot ausführbare jar-Datei zum Einsatz kommt, sind nach aktuellem Kenntnisstand nicht verwundbar. Da es sich jedoch um eine allgemeine Schwachstelle handelt, können weitere Wege zur Ausnutzung nicht ausgeschlossen werden.

Für die Produkte Operation Scheduler und SiPass integrated stehen bereits Updates zur Verfügung. Für die aktuell unterstützen Versionen von Siveillance Identity ist dies noch **nicht** der Fall.

Update 1:
Seit dem 27.04.2022 stehen Updates für das Produkt Siveillance Identity in den Versionen 1.5 und 1.6 zur Verfügung.

Bewertung

Das BSI geht – unter anderem aufgrund der Verbreitung im KRITIS-Sektor Transport und Verkehr – von einer grundsätzlichen Relevanz aus. Der Einsatz der Software in anderen Bereichen der deutschen Wirtschaft oder Verwaltung kann nicht ausgeschlossen werden.

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Dem BSI liegen öffentliche Berichte vor, dass die zugrundeliegende Schwachstelle Spring4Shell bereits aktiv ausgenutzt wird [TRM2022]. Daher ist von einer erhöhten Bedrohungslage auszugehen.

Maßnahmen

Das BSI empfiehlt jedem Betreiber zu überprüfen, ob die betroffenen Produkte im Einsatz sind und die von Siemens beschriebenen Maßnahmen [SIE2022] zeitnah zu berücksichtigen. Unter Beachtung der jeweiligen Risikoabwägung sollten vorhandene Systeme schnellstmöglich auf die vom Hersteller bereitgestellten, nicht-verwundbaren Versionen aktualisiert werden.

Für nicht-patchbare Systeme oder Software, für die kein Update zur Verfügung steht, müssen mindestens ein- und ausgehende Verbindungen mit dem Internet unterbunden werden. Unter Beachtung der jeweiligen Risikoabwägung sollte eine Isolierung der Systeme und eine engmaschige Überwachung in Erwägung gezogen werden.

Es ist davon auszugehen, dass grundsätzlich auch noch weitere IT-Komponenten für Spring4Shell anfällig sind. Daher empfiehlt das BSI dringend, regelmäßig die Sicherheitshinweise von allen IT-Herstellern, deren Produkte in der eigenen Organisation zum Einsatz kommen, zu prüfen.

Links

[SIE2022] SSA-254054: Spring Framework Vulnerability (Spring4Shell or SpringShell, CVE-2022-22965) - Impact to Siemens Products
https://cert-portal.siemens.com/productcert/pdf/ssa-254054.pdf

[TRM2022] CVE-2022-22965: Analyzing the Exploitation of Spring4Shell Vulnerability in Weaponizing and Executing the Mirai Botnet Malware
https://www.trendmicro.com/en_us/research/22/d/cve-2022-22965-analyzing-the-exploitation-of-spring4shell-vulner.html