Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Spring4Shell-Schwachstelle in Zutrittskontrollsystemen von Siemens

CSW-Nr. 2022-215640-1132, Version 1.1, 29.04.2022

IT-Bedrohungslage*: 2 / Gelb

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.

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.

* 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.

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.

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

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs) welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

   Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

2) Welche Einstufungen existieren?

   - **TLP:WHITE: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
     Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.