Cybersecurity – Mitteilung

Security Advisory zur Bewertung von Common Vulnerabilities and Exposures (CVE)

SimServ, Chargenviewer, SiCon, ISA

MMM Münchener Medizin Mechanik GmbH
Semmelweisstraße 6
D-82152 Planegg
www.mmmgroup.com

Stand: 2022-01-12, rev. 03

1 Einleitung

Hersteller von Medizinprodukten oder von Softwareprodukten, die in ein Krankenhausnetzwerk eingebunden wird, sowie Betreiber von IT-Netzwerken, in die Medizinprodukte / Softwareeingebunden werden, sind als Akteure gleichermaßen beteiligt, um Risiken für Patienten, Anwender und Dritte durch die Einbindung von Medizinprodukten in Netzwerke zu beherrschen.

Das Bundesamt für Sicherheit in der Informationstechnik BSI warnt in diesem Zusammenhang vor relevanten Schwachstellen bei IT-Systemen.

Das BSI überwacht dabei u.a. die globale Datenbank für Common Vulnerabilities and Exposures (CVE) [cve.mitre.org].In dieser Datenbank werden systematisch neue Sicherheitslücken mit einem eindeutigen CVE-Code, der „CVE-ID number“ zusammen mit einer Kurzbeschreibung der Sicherheitslücke und Referenzen zu entsprechenden Reports veröffentlicht.

Die Liste der Common Vulnerabilities and Exposures wird von der Mitre Corporation in Zusammenarbeit mit den „CVE Numbering Authorities“ bestehend aus Sicherheitsexperten, Bildungs-einrichtungen, Behörden und Herstellern von Sicherheitssoftware gepflegt.

Wenn BSI zum Schutz der kritischen Infrastrukturen wie z.B. Kliniken explizit vor veröffentlichten aus Sicht des BSI kritischen Sicherheitslücken warnt, können daraus ggf. Fragen zu Produkten der MMM Münchener Medizin Mechanik GmbH entstehen.

Vorliegende Mitteilung wird zu speziellen Warnungen des BSI zur Weitergabe an Kunden der MMM erstellt.

2 Geltungsbereich dieser Sicherheits - Mitteilung

Dieses Dokument gilt für MMM Software, die mit der MMM RUMED360® Software **SimServ**, **Chargenviewer**, **SiCon** oder **ISA** ausgestattet sind.

- Die MMM Middleware **SimServ** (RUMED360® Cycles) wird als Dienst auf dem Server betrieben. SimServ kommuniziert mit dem eingebundenen Medizinprodukt (Sterilisatoren und Reinigungs- und Desinfektionsgeräte) und legt die Chargendaten dieser

Geräte in einem definierten Verzeichnis ab, aus dem diese entweder von einer weiteren Anwendung verarbeitet werden können oder zu Datensicherungszwecken gespeichert werden.

- Die MMM Software **ChargenViewer** (RUMED360® Cycles View) wird als Programm auf dem Desktop von Krankenhausmitarbeitern (AEMP, Administrator, …) betrieben. ChargenViewer ist ein Software-Programm zum Betrachten, Ausdrucken und Exportieren von Zyklusdaten von MMM Sterilisatoren und MMM RDG.

- Die MMM Software **ISA** (Intelligent Service Advisor; RUMED360® ISA) wird als optionaler Dienst auf dem Server betrieben. Der ISA Server erweitert Baureihen der MMM um die Fähigkeit E-Mails mit hilfreichen Informationen zu verschicken. Wartungsinformationen erinnern rechtzeitig an durchzuführende Service-Arbeiten an der Maschine. Es gibt Informationen, die automatisch von der Maschine verschickt werden und solche, die auf Anforderung eines Bedieners verschickt werden.

- Die MMM Software **SiCon** (RUMED360® Sicon) wird als optionaler Dienst auf einem Industrie PC betrieben, der mit den MMM Baureihen Vakulab HL und Fluipharm HL geliefert wird. SiCon erweitert die genannten Geräte, um die Fähigkeit Zyklusdaten aktiv an SimServ zu übertragen bzw. auszudrucken.

Dieses Dokument gilt NICHT für MMM Medizinprodukte, die mit der MMM Software **Sterisecure, Hypersoft, Formsoft** oder **Washersoft** ausgestattet sind.

- **WasherSoft** ist der Name der Software für die Geräte der Baureihen Uniclean ML und Uniclean PL II.

- **Sterisecure** ist der Name der Software für die Geräte der Baureihen Selectomat PL und Vacudes PL.

- **Hypersoft** ist der Name der Software für die Geräte der Baureihe Hyper LTS.

- **Formsoft** ist der Name der Software für die Geräte der Baureihe Formomat PL.

3 BSI – Informationen zur Sicherheitslücke (Vulnerability)

Informationen durch das Bundesamt für Sicherheit in der Informationstechnik BSI:

„Die kritische Schwachstelle (Log4Shell) in der weit verbreiteten Java-Bibliothek Log4j führt nach Einschätzung des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu einer extrem kritischen Bedrohungslage. Das BSI hat daher seine bestehende Cyber-Sicherheitswarnung auf die Warnstufe Rot hochgestuft. Ursächlich für diese Einschätzung ist die sehr weite Verbreitung des betroffenen Produkts und die damit verbundenen Auswirkungen auf unzählige weitere Produkte. Die Schwachstelle ist zudem trivial ausnutzbar, ein Proof-of-Concept ist öffentlich verfügbar. Eine erfolgreiche Ausnutzung der Schwachstelle ermöglicht eine vollständige Übernahme des betroffenen Systems. Dem BSI sind welt- und deutschlandweite Massen-Scans sowie versuchte Kompromittierungen bekannt. Auch erste erfolgreiche Kompromittierungen werden öffentlich gemeldet.

Das ganze Ausmaß der Bedrohungslage ist nach Einschätzung des BSI aktuell nicht abschließend feststellbar. Zwar gibt es für die betroffene Java-Bibliothek Log4j ein Sicherheits-Update, allerdings müssen alle Produkte, die Log4j verwenden, ebenfalls angepasst werden. Eine Java-Bibliothek ist ein Software-Modul, das zur Umsetzung einer bestimmten Funktionalität in weiteren Produkten verwendet wird. Es ist daher oftmals tief in der Architektur von Software-Produkten verankert. Welche Produkte verwundbar sind und für welche es bereits Updates gibt, ist derzeit nicht vollständig überschaubar und daher im Einzelfall zu prüfen. Es ist zu erwarten, dass in den nächsten Tagen weitere Produkte als verwundbar erkannt werden.“

Das BSI warnte am 11.12.2021 erstmals vor dieser kritischen Schwachstelle.

Details zu den Sicherheitslücken

Es wurden im Zusammenhang mit **Log4Shell** bzw. **Log4j** Sicherheitslücken auf cve.mitre.org dokumentiert.

Datum der Veröffentlichung durch BSI:
2021-12-11

https://cve.mitre.org
https://www.cve.org

CVE ID(s):
CVE-2021-44228 → Base Score = 10.0
CVE-2021-45046 → Base Score = 9.0
CVE-2021-45105 → Base Score = 5.9
CVE-2021-44832 → Base Score = 6.6

Risikobewertung der Sicherheitslücke:
Das Risiko bzw. der Schweregrad einer Sicherheitslücke (Vulnerability) wird i.d.R. mittels des CVSS Score bewertet. Das CVSS (Common Vulnerability Scoring System) ist ein Industriestandard zur Einstufung des Risikos von Sicherheitslücken in Software. Der Standard wird durch das Forum of Incident Response and Security Teams (FIRST) verwaltet; weitere Informationen zu CVSS finden Sie auf www.FIRST.org.

- **durch den Analyst**

  CVE-2021-44228

  CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

  10.0 KRITISCH

  https://nvd.nist.gov/vuln/detail/CVE-2021-44228

- **durch den Hersteller**

  Hersteller: Apache Software Foundation
  CVSS Base Score: 9.7 bzw. 9.8 [CVSS v3]

- **durch BSI**

  IT-Bedrohungslage*: 4 / Rot

4 Bewertung durch MMM

Die MMM Münchener Medizin Mechanik GmbH setzt die betroffene Bibliothek ein, jedoch mit anderen Rahmenbedingungen als die durch BSI / NIST angenommenen worst case Anwendungsszenarien.

Betroffene MMM Software Versionen:

- ChargenViewer < 1.38.4
- SimServ < 1.50.4
- SiCon < 1.3.4
- ISA < 2.0.2

Betroffene MMM Produkte und Baureihen:

KEINE.

Hinweis: Die Baureihen Vakulab HL und Fluipharm HL sind indirekt betroffen, wenn die Software SiCon auf dem mitgelieferten Industrie-PC installiert wurde. Die Betriebssoftware „SiSoft“ der beiden Baureihen ist nicht betroffen. Bei den beiden genannten Baureihen handelt es sich nicht um Medizinprodukte. Sie werden i.d.R. nicht in einem Krankenhaus bzw. einer „kritischen Infrastruktur“ betrieben.

Risikobewertung der Sicherheitslücke(n) durch MMM:

Der Schweregrad wird anhand des CVSS wie folgt ermittelt:

CVSS v3.1 Base Score Range	*Schweregrad*
0,0	kein Risiko vorhanden
0,1 - 3,9	niedrig
4,0 - 6,9	mittel
7,0 - 8,9	hoch
9.0 - 10.0	kritisch

https://www.first.org

- **CVSS v3.1 Base Score (MMM)**

  8,2

- **Schweregrad**

  High

Was müssen Sie tun?

Bitte setzen Sie sich mit dem MMM Support in Verbindung, falls Ihre Prüfung der IT-Sicherheit eine Aktualisierung ihrer Software erfordert.

MMM empfiehlt grundsätzlich dieses Update durchzuführen.

Kontakt: service@mmmgroup.com