ST. JUDE MEDICAL

Media Release

ANSPRECHPARTNER
St. Jude Medical GmbH
Astrid Tinnemans
Manager Public Relations
Helfmann-Park 7
65760 Eschborn

Tel. +49-6196-77 11 142
E-Mail: atinnemans@sjm.com

St. Jude Medical weist von Muddy Waters erhobene Sicherheitsvorwürfe zurück und bekräftigt die Sicherheit seiner Produkte und sein Eintreten für die Patientensicherheit

Analyse des Sicherheitsprotokolls von St. Jude Medical bestätigt das Funktionieren hochentwickelter technischer Sicherheitssysteme zum Schutz des Patienten

Eschborn, den 30. August 2016 – St. Jude Medical, ein weltweit tätiges Medizintechnik-Unternehmen, gab heute folgendes Statement ab: Wir haben die am 25. August 2016 von Muddy Waters Capital und MedSec erhobenen Vorwürfe in Bezug auf die Sicherheit unserer Herzschrittmacher und Defibrillatoren geprüft. Uns wäre es lieber gewesen, wir hätten die Möglichkeit gehabt, die fraglichen Informationen in allen Einzelheiten einzusehen. Jedoch kommen wir auch aufgrund der uns verfügbaren Informationen zu dem Schluss, dass der Bericht falsch und irreführend ist.

Unsere oberste Priorität ist es nun, allen Patienten, Betreuern und Ärzten die Gewissheit zu geben, dass unsere Produkte sicher sind, und sie darin zu bestärken, weiterhin die erwiesenen klinischen Vorzüge der Fernüberwachung zu nutzen. St. Jude Medical steht zur Sicherheit seiner Produkte, die auch von unabhängigen Dritten bestätigt und von unseren zulassungsrechtlichen Einreichungen gestützt wird.

Die Fernüberwachung stellt für den Patienten eine sichere und effektive Methode dar, um mit dem Arzt zu kommunizieren. In führenden Publikationen ist bestens dokumentiert, dass die Fernüberwachung Leben rettet. Wir von St. Jude Medical arbeiten mit externen Experten, Forschern, Behörden und Regulierungsstellen für Cybersicherheit zusammen, um im Rahmen der Entwicklung und während des gesamten Lebenszyklus unserer Produkte geeignete Schutzmechanismen für unsere Daten und Produkte zu entwickeln.

Diese Experten unterstützen uns bei der Gestaltung von Sicherheitskontrollen von den frühen Phasen des Produktdesigns bis hin zur abschließenden Freigabe und laufenden Produktoptimierung; hierzu gehören unter anderem Software-Updates und Sicherheits-Patches für unsere Produkte.

Auch führen wir nach Leitlinien der FDA und unter Mitwirkung von internen und externen Experten regelmäßig Gefährlichkeitsanalysen und Penetrationstests durch. Darüber hinaus arbeiten wir mit Branchen- und Regierungsorganisationen zusammen, um Einblicke in neueste Trends zu erhalten und entsprechend auf diese zu reagieren.

Unser System stellt einen automatisierten Prozess für die Remote-Aktualisierung aller aktiv genutzten Merlin@home Systeme bereit, damit Sicherheitsoptimierungen bei Verfügbarwerden automatisch eingespielt werden. Merlin@home Systeme, die nicht aktiv genutzt werden und mit dem Internet verbunden sind, werden bei Verfügbarwerden eines neuen Updates ebenfalls aktualisiert, sobald sie wieder genutzt werden.

Unsere Analyse kam zu dem Schluss, dass sich die Mehrzahl der in dem Bericht aufgeführten Beobachtungen auf ältere Versionen der Merlin@home™ Geräte bezieht (d. h. solche, die nicht durch das automatisierte Remote-Upgradeverfahren aktualisiert wurden).

Wir vertrauen auf die von uns bereitgestellte Technologie und auf unseren Prozess, bei dem wir kontinuierlich auf unsere Sicherheitsprotokolle und -prozesse bauen. Wir möchten unseren Patienten die Gewissheit geben, dass unsere Systeme den höchsten internationalen Sicherheitsanforderungen entsprechen, wie sie von Regulierungsbehörden und internationalen Normungsorganisationen vorgegeben werden.

Die Behauptung zu einer aus der Ferne bewirkten Batterieentladung ist irreführend
In dem Bericht wurde behauptet, die Batterie könne aus einer Distanz von 50 Fuß (15 m) entladen werden. Dies ist nicht möglich, da die Reichweite der drahtlosen Kommunikation nach erfolgter Einsetzung des Implantats ungefähr 7 Fuß (2,1 m) beträgt. Hier stellt sich nun grundsätzlich die Frage nach der Prüfmethodik, die als Grundlage für den Bericht von Muddy Waters Capital und MedSec diente.

Zudem müssten bei dieser Distanz im beschriebenen Szenario über hunderte von Stunden hinweg unablässig „Ping"-Befehle übermittelt werden. Um es klar auszudrücken: Ein Patient dürfte sich mehrere Tage lang nicht von der Stelle bewegen, und der Hacker dürfte sich nicht weiter als 7 Fuß vom Patienten weg bewegen. Sollte dieser unwahrscheinliche Fall dennoch eintreten, verfügen die Implantate über einen Vibrationsalarm, der den Patienten warnt, wenn der Ladestand der Batterie unter einen bestimmten Pegel abfällt.

Die fehlerbehaftete Prüfmethodik und ihre Anwendung bei veralteter Software offenbart einen grundlegenden Mangel an Verständnis für die Technik medizinischer Geräte.
Im Bericht wurde behauptet, das System könne ähnlich wie beim „Absturz" eines Computersystems in Mitleidenschaft gezogen werden. Zu dieser Simulation enthält der Bericht nur wenige Einzelheiten, dafür jedoch viele Widersprüche. Die Bildschirmaufnahme des Merlin Programmiergeräts im Bericht von Muddy Waters zeigt jedenfalls ein normal funktionierendes Implantat. Die roten Elemente am Bildschirm lassen erkennen, dass keine Elektroden an das Implantat angeschlossen sind.

Das Implantat stimuliert einwandfrei mit den programmierten 40 Schlägen pro Minute. Die Bildschirmaufnahme zeigt das zu erwartende Verhalten des SecureSense-Algorithmus, wenn das Implantat ohne angeschlossene Elektroden eine Stimulation abgibt.

St. Jude Medical wird stets wachsam bleiben und sich für Patientensicherheit einsetzen
Unsere Software wurde von verschiedenen unabhängigen Organisationen und Forschungseinrichtungen bewertet und beurteilt, so etwa von Deloitte und Optiv. Darüber hinaus erhielt Merlin.net durch ein internes Audit bei St. Jude Medical im Jahr 2013 und in allen Folgejahren die Safe Harbor-Zertifizierung. Dies beinhaltet ein jährliches Audit der zentralen Sicherheitskontrollen innerhalb der Merlin.net Umgebung.

Zudem hat Merlin.net seit dem Jahr 2009 ununterbrochen die Zertifizierung nach ISO 27001 erhalten. Dies beinhaltet wiederum ein internes Audit der Sicherheitskontrollen und eine unabhängige Zertifizierung durch eine dritte Stelle, nämlich das BSI. Im Jahr 2015 haben wir eine Höherstufung auf die Zertifizierung nach ISO 27001:2013 erfolgreich abgeschlossen.

Muddy Waters stellt außerdem zahlreiche haltlose Behauptungen auf, die rein spekulativ sind und durch keinerlei Beweise belegt sind. Hierzu gehört die angebliche Möglichkeit, beliebige Geräte von SJM zu imitieren, durch Zurückentwicklung ein Programmiergerät im Taschenformat herzustellen, oder einen groß angelegten Angriff über das Merlin-Netzwerk auszuführen. Uns sind jedoch keinerlei Bedrohungen dieser Art bekannt. Wir bleiben jedoch wie immer wachsam gegenüber jenen, die mit immer größer werdender Raffinesse den Zugriff auf Geräte/Daten zu erlangen versuchen, und werden uns beim Bekanntwerden entsprechender Informationen etwaigen Problemen umgehend stellen.

Wir wissen, wie wichtig es ist, dass Ärzte zeitnah und in verantwortungsvoller Weise mit aktuellen und akkuraten Informationen versorgt werden, um fundierte Entscheidungen zur Behandlung ihrer Patienten treffen zu können. Unsere Analyse zeigt abermals, wie wichtig es ist, dass Forscher und Hersteller zusammenarbeiten, um potenzielle Probleme gemeinsam zu besprechen, zu lösen und dadurch jede unnötige Verängstigung der Patienten zu vermeiden.

St. Jude Medical ist ein erklärter Befürworter der verantwortungsvollen Offenlegung und arbeitet proaktiv mit Industrieorganisationen wie NH-ISAC und ICS-CERT zusammen.
Wir möchten jeden, der Fragen zur Produktsicherheit hat, dazu ermuntern, unter **productsecurity@sjm.com** mit uns Kontakt aufzunehmen. Wir möchten jeden, der bei einem Produkt von St. Jude Medical eine potenzielle Schwachstelle in Bezug auf die Cybersicherheit vermutet, darum bitten, unter **vulnerabilityreporting@sjm.com** mit uns Kontakt aufzunehmen, um eine genauere Untersuchung und Analyse zu ermöglichen. Nur so können wir entsprechende Informationen im Interesse der Patientensicherheit validieren und kommunizieren.

Die Patientensicherheit war schon immer unsere oberste Priorität, und wir haben allen Grund zu glauben, dass unsere Produkte sicher sind. Da uns bewusst ist, dass die Cybersicherheit für unsere Patienten ein großes Anliegen darstellt, nimmt sie auch für St. Jude Medical einen hohen Stellenwert ein. Auf unserer Website sjm.com haben wir eigens hierfür eine Ressource geschaffen, um unser entschlossenes Eintreten für Produkt- und Informationssicherheit zu unterstreichen.

Über die Auswirkungen des St. Jude Medical Portfolios für Fernüberwachung
Das St. Jude Medical Merlin.net Patient Care Network (PCN) ist ein preisgekröntes Hochfrequenz-(HF-) Fernüberwachungssystem, das dazu dient, die Behandlungsergebnisse bei Patienten mit Herzschrittmachern, implantierbaren Kardioverter-Defibrillatoren (ICD) und Defibrillatoren für die kardiale Resynchronisationstherapie (CRT-Ds) zu verbessern. Ärzte können über die sichere Merlin.net PCN Website in Sekundenschnelle auf die Daten der bei ihren Patienten eingesetzten Implantate zugreifen und diese aus der Ferne beobachten und beurteilen, um etwaige Interventionen festlegen zu können. Forschungen aus jüngerer Zeit haben gezeigt, dass sich die Überlebensrate durch Fernüberwachung verbessern lässt und gleichzeitig Klinikeinweisungen sowie die Inanspruchnahme des Gesundheitswesens durch die Patienten reduziert werden.

Im Jahr 2008 verbesserte St. Jude Medical die außergewöhnlich hohe Sicherheit des Merlin.net PCN noch einmal durch die Einführung des Merlin@home™ Transmitters. Dieser ermöglicht ein effizientes Management der medizinischen Versorgung aus der Ferne und bietet Ärzten zusätzliche Optionen für eine frühzeitige Intervention und größere Versorgungseffizienz. Die von Merlin@home übermittelten Daten sind vollständig verschlüsselt und erfüllen oder übertreffen alle geltenden Anforderungen an den Datenschutz und die Datensicherheit, und zwar in allen Ländern, in denen das Merlin.net PCN verwendet wird. Außerdem war das Merlin.net PCN das erste System zur Überwachung kardialer Implantate, dem die Zertifizierung nach der strengen, weltweit gültigen Datensicherheitsnorm ISO/IEC 27001:2005 verliehen wurde, und unsere Zertifizierung wird fortlaufend auditiert, aktualisiert und erneuert.

Die Fernüberwachung von Herzpatienten wurde im letzten Jahrzehnt zu einer Best Practice. Im Jahr 2016 hat die Heart Rhythm Society in ihren jüngsten Richtlinien die Fernüberwachung zum Versorgungsstandard erklärt. St. Jude Medical hat mit seinem HF Merlin.net Patient Care Network (PCN) und dem Patientensystem Merlin@Home für diese lebensrettende Möglichkeit Pionierarbeit geleistet. Dutzende von Studien belegen auch weiterhin die positiven Auswirkungen dieser Technik auf die Behandlungsergebnisse und die Senkung der Kosten für das Gesundheitswesen.

Patienten, die Fragen zu Möglichkeiten der Fernversorgung von St. Jude Medical haben, können unsere Abteilung Remote Care Services unter der Rufnummer 1-877-MY MERLIN (1-877-696-3754) kontaktieren.

Über St. Jude Medical
St. Jude Medical ist ein weltweit führender Hersteller von medizintechnischen Geräten, der es sich zum Ziel gesetzt hat, bei der Behandlung einiger der teuersten Volkskrankheiten der Welt neue Wege zu gehen. Dazu entwickelt das Unternehmen kosteneffiziente medizinische Technologien, die für Patienten in aller Welt lebensrettend sind und die Lebensqualität verbessern.

Von seinem Hauptsitz in St. Paul, Minn. (USA) aus agiert St. Jude Medical in fünf zentralen Bereichen: Herzinsuffizienz, Vorhofflimmern, Neuromodulation, klassische Rhythmologie und Herz-Kreislauf-Krankheiten.

Weitere Informationen erhalten Sie unter **www.sjm.de** und **www.sjm.com,** oder folgen Sie uns via Twitter: **@SJM_Media.**

Zukunftsgerichtete Aussagen
Diese Pressemitteilung enthält zukunftsgerichtete Aussagen im Sinne des Private Securities Litigation Reform Act von 1995, die Risiken und Ungewissheiten enthalten. Solche zukunftsgerichteten Aussagen umfassen die Erwartungen, Pläne und Aussichten für das Unternehmen, inklusive potenzielle klinische Erfolge, erwartete behördliche Genehmigungen und zukünftige Produkteinführungen sowie geplante Erträge, Margen, Gewinne und Marktanteile.

Die Aussagen des Unternehmens basieren auf den aktuellen Erwartungen der Geschäftsführung und unterliegen bestimmten Risiken und Unsicherheiten, die dazu führen können, dass die tatsächlichen Ergebnisse von den in den zukunftsgerichteten Aussagen beschriebenen Ergebnissen abweichen.

Zu diesen Risiken und Ungewissheiten zählen Marktbedingungen und weitere Faktoren außerhalb des Einflussbereichs des Unternehmens sowie die Risikofaktoren und andere Warnhinweise, die in den Einreichungen des Unternehmens bei der US-Börsenaufsichtsbehörde SEC beschrieben werden. Dazu gehören auch die Faktoren und Hinweise, die in den Abschnitten „Risk Factors“ und „Cautionary Statements“ im Jahresbericht des Unternehmens auf Formblatt 10-K für das Geschäftsjahr bis zum 03. Januar 2015 und auf Formblatt 10-Q für das Geschäftsquartal bis zum 02. Juli 2016 aufgelistet werden. Das Unternehmen plant keine Aktualisierung dieser Aussagen und verpflichtet sich unter keinen Umständen dazu, jemandem eine solche Aktualisierung zukommen zu lassen.

Hinweis
Die Ausgangssprache, in der der Originaltext veröffentlicht wird, ist die offizielle und autorisierte Version. Übersetzungen werden zur besseren Verständigung mitgeliefert. Nur die Sprachversion, die im Original veröffentlicht wurde, ist rechtsgültig. Gleichen Sie deshalb Übersetzungen mit der originalen Sprachversion der Veröffentlichung ab.