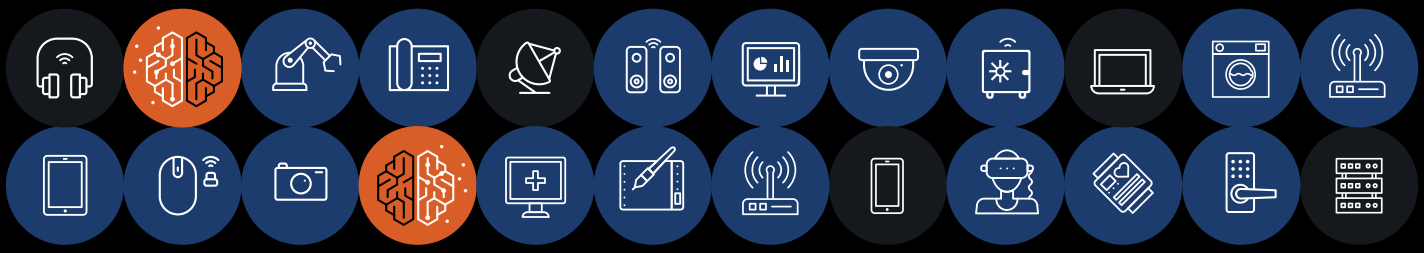
FORESCOUT
Active Defense for the Enterprise of Things™

AMNESIA:33

Kurzfassung zum Forschungsbericht



- Forescout Research Labs hat das Project Memoria gestartet. **Diese Initiative** soll die Community mit der **größten Untersuchung zur Sicherheit von TCP/IP-Stacks** unterstützen. Das Ziel von Project Memoria besteht darin, typische Schwachstellen in den TCP/IP-Stacks besser zu verstehen und die dadurch entstehenden Bedrohungen für das gesamte Unternehmensnetzwerk zu identifizieren und Maßnahmen zur Risikominderung aufzuzeigen.
- **AMNESIA:33** ist die erste Untersuchung, die wir im Rahmen von Project Memoria veröffentlicht haben. Wir stellen die Ergebnisse der Sicherheitsanalyse von sieben **Open-Source-TCP/IP-Stacks** vor und zeigen **33 neue Schwachstellen** in vier der sieben analysierten Stacks, die von großen IoT-, OT- und IT-Geräteherstellern verwendet werden.
- **Vier der Schwachstellen in AMNESIA:33 sind kritisch** und können auf bestimmten Geräten potenziell für Remote-Code-Ausführung ausgenutzt werden. Dadurch können Angreifer die Kontrolle über das Gerät übernehmen und es als Einfallstor in ein Netzwerk internetfähiger Geräte missbrauchen. Ebenso kann es für laterale Bewegungen innerhalb des Netzwerks dienen, als Brückenkopf im Zielnetzwerk oder als Endziel eines Angriffs. Für Unternehmen bedeutet das ein höheres Risiko von Netzwerkkompromittierungen oder böswilligen Akteuren, die den störungsfreien Geschäftsbetrieb bedrohen. Verbraucher müssen hingegen damit rechnen, dass ihre IoT-Geräte unbemerkt für große Angriffskampagnen wie Botnets missbraucht werden können.

Über 150

BETROFFENE HERSTELLER

forescout.com/amnesia33/ info-dach@forescout.com Telefon (weltweit): +1-408-213-3191

- AMNESIA:33 betrifft **mehrere Open-Source-TCP/IP-Stacks**, die **nicht nur einem bestimmten Unternehmen gehören**. Deshalb verbreiten sich einzelne Schwachstellen **unbemerkt und mühelos** über mehrere Codebasen, Entwicklerteams, Unternehmen und Produkte, was die Patch-Verwaltung erheblich erschwert.
- Wir gehen davon aus, dass mehr als 150 Anbieter und Millionen von Geräten für AMNESIA:33 anfällig sind. Es ist jedoch **schwierig, den vollen Umfang** von AMNESIA:33 zu bemessen, da die anfälligen Stacks weit verbreitet (auf verschiedensten IoT-, OT- und IT-Geräten an unterschiedlichen Standorten), äußerst modular (mit Komponenten, Funktionen und Einstellungen in verschiedenen Kombinationen, wobei die Codebasen aufgespalten werden) und in undokumentierten, tief eingebetteten Subsystemen integriert sind. Aus dem gleichen Grund lassen sich diese Schwachstellen meist nur mit großem Aufwand schließen.
- Die von AMNESIA:33 betroffenen TCP/IP-Stacks finden sich in Betriebssystemen eingebetteter Geräte, in Systems-on-a-Chip (SoC, dt. Ein-Chip-System), Netzwerktechnik, OT-Geräten sowie in einer unüberschaubaren Zahl von IoT-Geräten aus dem Industrie- und Verbraucherbereich.
- TCP/IP-Stacks sind kritische Komponenten aller per IP-Adresse verbundenen Geräte (einschließlich IoT und OT), da sie für die grundlegende Netzwerkkommunikation verantwortlich sind. Eine Sicherheitslücke in einem TCP/IP-Stack kann extrem gefährlich sein, da der Code in diesen Komponenten **zur Verarbeitung *aller* eingehenden Netzwerkpakete dienen kann, die das Gerät erreichen**. Das bedeutet, dass einige Schwachstellen in einem TCP/IP-Stack auch ausgenutzt werden können, wenn das Gerät sich nur im Netzwerk befindet und keine Anwendungen ausführt.
- Ursache vieler Schwachstellen in **AMNESIA:33** sind mangelnde Sicherheitspraktiken bei der Software-Entwicklung, z. B. fehlende einfache Eingabevalidierungen. Diese Schwachstellen bestehen meist im Zusammenhang mit **Speicherbeschädigung** und können **Denial-of-Service-Angriffe, Informationslecks** oder **Remote-Code-Ausführung** ermöglichen.
- Aufgrund der Schwierigkeiten beim Identifizieren und Patchen anfälliger Geräte ist die Schwachstellen-verwaltung bei TCP/IP-Stacks eine große Herausforderung für die Sicherheits-Community. Wir empfehlen die **Implementierung von Lösungen, die einen detaillierten Überblick über alle Geräte im Netzwerk bieten**. Die Lösungen sollten die Überwachung der Netzwerkkommunikation ermöglichen und anfällige Geräte oder Netzwerksegmente isolieren, um die Risiken durch diese Schwachstellen zu minimieren.

Nicht nur alles sehen, sondern alles schützen.

Kontaktieren Sie uns noch heute, damit Sie Ihr Enterprise of Things aktiv verteidigen können.

Gesamten Bericht herunterladen (in englischer Sprache): Machen Sie sich mit den Details unserer Untersuchungen vertraut und erfahren Sie, welche Schutzmaßnahmen implementiert werden können.

Whitepaper herunterladen (in englischer Sprache): Erfahren Sie, wie Forescout Sie bei der Abwehr von AMNESIA:33 unterstützen kann und mit welchen sechs Best Practice-Maßnahmen Sie Ihr Unternehmen zuverlässig schützen können.

Webinar ansehen (in englischer Sprache): Unsere Experten stellen die wichtigsten Punkte der Untersuchung vor.

forescout.com/amnesia33/ info-dach@forescout.com Telefon (weltweit): +1-408-213-3191

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W. Tasman Dr.
San Jose, CA 95134 USA

E-Mail: info-dach@forescout.com
Telefon (weltweit): +1-408-213-3191
Support: +1-708-237-6591

Weitere Informationen finden Sie unter Forescout.de