Neues Trellix Advanced Research Center stellt fest: Rund 350.000 Open-Source-Projekte sind durch Sicherheitslücke in der Lieferkette gefährdet

München, 21. September 2022 – Trellix, Experte für Cyber-Sicherheit und Vorreiter auf dem Gebiet innovativer XDR-Technologien, gibt den Startschuss für sein Advanced Research Center (ARC) bekannt. Unter dem Dach des neuen Analysezentrums arbeiten Hunderte der weltweit renommiertesten Sicherheitsprofis und -wissenschaftler. Sie alle haben sich der Aufgabe verschrieben, aufschlussreiche und praxisrelevante Echtzeit-Erkenntnisse bereitzustellen, von denen Trellix-Kunden als auch die Branche als Ganzes profitieren können.

Das Trellix Advanced Research Center verfolgt eine der umfassendsten Agenden der Cyber-Sicherheitsindustrie und setzt sich zum Ziel, sicherheitsrelevante Trends frühzeitig zu identifizieren und Trellix-Kunden wie -Partnern mit Rat und Tat zur Seite zu stehen. Die Fünf-Punkte-Richtlinie des ARC umfassen die Bereiche Produktforschung und -entwicklung, Bedrohungsaufklärung, Resilienz gegenüber kriminellen Angreifern und Interessensvertretern sowie Forschungstechnik und Datenwissenschaft. Basierend auf dem Trellix „Data Lake“ wird das Analysezentrum Berichte, Forschungsergebnisse und Erkenntnisse zu aktuellen Methoden, Trends und Akteuren in der Bedrohungslandschaft veröffentlichen und zugleich über die F&E-Aktivitäten von Trellix berichten sowie darüber informieren, wie Trellix-Lösungen bei der Abwehr vor Bedrohungen unterstützen können.

Weitere Informationen finden Sie im Blog zum Trellix Advanced Research Center und im Trellix Threat Center.

Sicherheitslücke in Phyton-Tar-Datei verdeutlicht Komplexität der Software-Lieferkette

Gleich zu Beginn seiner Tätigkeit veröffentlicht das Trellix Advanced Research Center detaillierte Informationen zu CVE-2007-4559, einer Sicherheitslücke, von der nicht nur über 350.000 Open-Source-, sondern auch Closed-Source-Projekte betroffen sein dürften. Die Schwachstelle befindet sich im Python-Modul für Tar-Dateien, einem Standardmodul in allen Projekten, die Python verwenden, und ist in den Frameworks von Netflix, AWS, Intel, Facebook und Google sowie in Anwendungen für Machine Learning, Automatisierung und Docker-Containerisierung weit verbreitet. Durch das Hochladen einer bösartigen Datei kann die Sicherheitslücke ausgenutzt werden, die mit zwei oder drei Zeilen einfachen Codes generiert wird und Angreifern möglicherweise die Ausführung beliebigen Codes oder die Kontrolle über ein Zielgerät ermöglicht.

„Wenn wir von Bedrohungen der Software-Lieferkette sprechen, meinen wir meist Cyber-Angriffe wie SolarWinds. Dabei sollte uns längst klar sein, dass ein schwaches Code-Fundament ernste Auswirkungen auf die Sicherheit der darauf aufbauenden Programme haben kann“, erklärt **Christiaan Beek, Head of Adversarial & Vulnerability Research bei Trellix**. „Viele IT-Handbücher und Online-Schulungsmaterialien ignorieren diese Gefahr und sorgen so dafür, dass die Sicherheitslücke über Jahre bestehen bleibt. Es ist daher extrem wichtig, Entwickler über alle Schichten des Technologie-Stacks aufzuklären, damit Bedrohungen aus der Vergangenheit nicht erneut virulent werden können.“

Open-Source-Programme wie Python sind unverzichtbare Instrumente zur Förderung von Innovationen im IT-Sektor. Für einen zuverlässigen Schutz vor bekannten Gefahren braucht es daher die Zusammenarbeit aller Beteiligten aus der gesamten Branche. Trellix selbst setzt auf die Code-Übernahme über einen GitHub Pull Request, um Open-Source-Projekte effektiv zu schützen. Auf der GitHub-Seite des Trellix Advanced Research Center finden Entwickler ein Tool, mit dem sie ihre Anwendungen auf den Bug überprüfen können.

Weitere Informationen:

- Trellix Threat Center
- Tarfile: Exploiting the World With a 15-Year-Old Vulnerability
- Open-Source Intelligence to Understand the Scope of N-Day Vulnerabilities
- Limiting the Software Supply Chain Attack Surface
- Trellix GitHub

Quelle: Trellix

###

Über das Trellix Advanced Research Center

Unter dem Dach des Trellix Advanced Research Center (ARC) finden sich zahlreiche renommierte Cybersecurity-Profis und -Wissenschaftler. Sie alle haben sich der Aufgabe verschrieben, aufschlussreiche und praxisrelevante Echtzeiterkenntnisse bereitzustellen, von denen Trellix-Kunden und die Branche als Ganzes profitieren können. Gestützt auf eine der ambitioniertesten Agenden der Cybersecurity-Industrie arbeiten sie unermüdlich daran, sicherheitsrelevante Trends frühzeitig aufzuspüren und Trellix-Kunden wie -Partnern mit Rat und Tat zur Seite zu stehen. Weitere Informationen finden Sie unter https://www.trellix.com/en-us/threat-center.html.

Über Tellix

Trellix ist ein globales Unternehmen, das die Zukunft der Cyber-Sicherheit neu definiert. Die offene und native Extended Detection and Response (XDR)-Plattform verhilft Unternehmen, die sich modernen, fortschrittlichen Cyber-Bedrohungen gegenübersehen, zu einem höheren Vertrauen in den Schutz und der Resilienz ihres Geschäftsbetriebs. In Kombination mit dem umfangreichen Partner-Ökosystem sind Sicherheitsexperten von Trellix in der Lage, die technologischen Innovationsprozesse seiner über 40.000 Geschäfts- und Regierungskunden mithilfe von Datenwissenschaft (Data Science) und Automatisierung zu beschleunigen. Weitere Informationen finden Sie unter www.trellix.com.

Pressekontakt

Ina Rohe/ Tobias Petermichl

Emil Riedel Str. 18

80538 München

irohe@hoffman.com