tenable.ot

LÖSUNGSÜBERSICHT

SCHWACHSTELLEN-MANAGEMENT MIT TENABLE.OT

MANAGEMENT VON OT-SCHWACHSTELLEN

OT-Umgebungen werden oft als Lebensnerv von kritischen Infrastrukturen und Produktionsanlagen betrachtet. Sie setzen sich aus speicherprogrammierbaren Steuerungen (SPS), Mensch-Maschine-Schnittstellen (HMI), verteilten Steuerungssystemen (DCS) sowie IT-Assets zusammen und werden zunehmend komplexer. Durch die schnelle Einführung von IoT-Technologien sowie die Konvergenz von IT und OT sind diese Umgebungen anfälliger für Cyberrisiken und Bedrohungen geworden.

Einer der Hauptangriffsvektoren für OT sind Schwachstellen. Ähnlich wie IT-Umgebungen können auch in OT-Umgebungen regelmäßig neu aufgedeckte Schwachstellen vorliegen, die ständiger Aufmerksamkeit bedürfen. Doch im Gegensatz zu IT-Umgebungen gibt es in OT-Umgebungen unter Umständen weniger Wartungsfenster, in denen diese Schwachstellen behoben werden können. Tenable.ot löst dieses Problem durch seine Schwachstellen-Management-Funktion mit VPR-Bewertung (Vulnerability Priority Rating).

ASSET-BESTANDSAUFNAHME

Tagtäglich veröffentlichen Forscher neue Schwachstellen in OT-Geräten und -Software. Allerdings wird ein Großteil davon für Ihr Unternehmen nicht von Belang sein, da Sie das spezifische Fabrikat und Modell nicht besitzen oder Ihre Firmware-Version nicht betroffen ist. Aus diesem Grund sollten Sie stets ein aktuelles Bestandsverzeichnis darüber besitzen, was genau in Ihrer OT-Umgebung vorhanden ist.

Tenable.ot nimmt eine Asset-Bestandsaufnahme vor, die den Echtzeit-Status der IT- und OT-Assets in Ihrer Umgebung wiedergibt und detaillierte Informationen bis hin zu Firmware, Kontaktplänen und Backplane für jedes einzelne Asset liefert. Diese Detailtiefe verbessert Ihre Sicherheitslage und bietet Ihnen darüber hinaus die Möglichkeit, eine vollständige und präzise Liste der Schwachstellen zu führen, die für spezifische Ausrüstung in Ihrer Umgebung relevant sind.

PRIORISIERUNG VON SCHWACHSTELLEN MITTELS VPR

Die NVD stellt CVSS-Bewertungen zur Verfügung, die den allgemeinen relativen Schweregrad einer Schwachstelle im Verhältnis zu anderen veröffentlichten Schwachstellen angeben, für die Exploits verfügbar sind. Die CVSS-Bewertung berücksichtigt allerdings nicht, wie sich die betreffende Schwachstelle auf Ihre spezifische Umgebung auswirken kann. Eine bestimmte Schwachstelle kann eine niedrige CVSS-Bewertung aufweisen, doch aufgrund anderer dynamischer

WICHTIGE VORTEILE

- **Die Asset-Bestandsaufnahme** erstellt in Echtzeit eine stets aktuelle Bestandsliste der Assets in Ihren Umgebungen. Dies erleichtert die Identifizierung der für Sie relevanten Schwachstellen.
- **Gehen Sie gezielt gegen Schwachstellen vor**, für die bereits Exploits vorliegen. Dank umfassender Informationen zu den Assets in Ihrem Netzwerk werden nur solche Schwachstellen angezeigt, die für Ihre Umgebung relevant sind.
- **Vollständige Abdeckung** bedeutet, dass Sie einen kompletten Überblick über sämtliche Assets und deren Schwachstellen in Ihrer Umgebung erhalten – ganz gleich, ob diese IT-, OT- oder IoT-basiert sind.
- **Die priorisierte Bewertung** mit Vulnerability Priority Rating (VPR) kombiniert von Tenable gesammelte Schwachstellendaten mit Daten zu Schwachstellen und Bedrohungen von Drittanbietern und analysiert diesen Datenbestand mit dem fortschrittlichen datenwissenschaftlichen Algorithmus, der von Tenable Research entwickelt wurde.

Informationen (z. B. der Reifegrad des Exploit-Codes oder das Auftreten bestimmter Bedrohungsereignisse im Zusammenhang mit einer Schwachstelle) ist die VPR-Bewertung im Allgemeinen relevanter. Daher stellt Tenable.ot sowohl eine CVSS-Bewertung als auch eine VPR-Bewertung zusammen mit sämtlichen Details bereit. Dies hilft Ihnen zu priorisieren, um welche Schwachstellen Sie sich während eines Wartungsfensters zuerst kümmern sollten und welchen Schwachstellen möglicherweise eine niedrigere Priorität eingeräumt werden kann.

FRÜHZEITIGE WARNUNG VOR POTENZIELLEN EXPLOITS

Es ist nicht ungewöhnlich, dass Bedrohungsakteure eine Schwachstelle bereits vor der NVD-Publikation angreifen. Da es bei der Veröffentlichung zu Verzögerungen kommen kann, ist Vorsicht geboten, wenn Sicherheitsfachkräfte die NVD als Single Source of Truth für Schwachstelleninformationen verwenden. Die VPR-Funktion stuft neue Schwachstellen zeitnah ein: 84 % der neuen Schwachstellen erhalten innerhalb eines Tages nach Bekanntwerden und 93 % innerhalb der ersten Woche eine VPR-Bewertung. Mithilfe des VPR können Sie Ihre Angriffsoberfläche reduzieren, indem Sie bereits vor der NVD-Veröffentlichung Schwachstellen beseitigen, die aktiv ausgenutzt werden.

FUNKTIONSWEISE

Priorisierung wird jede Nacht für mehr als **109.000 separate Schwachstellen berechnet**.

→ Das Modell sagt vorher, ob eine Schwachstelle in **naher Zukunft** ausgenutzt werden wird.

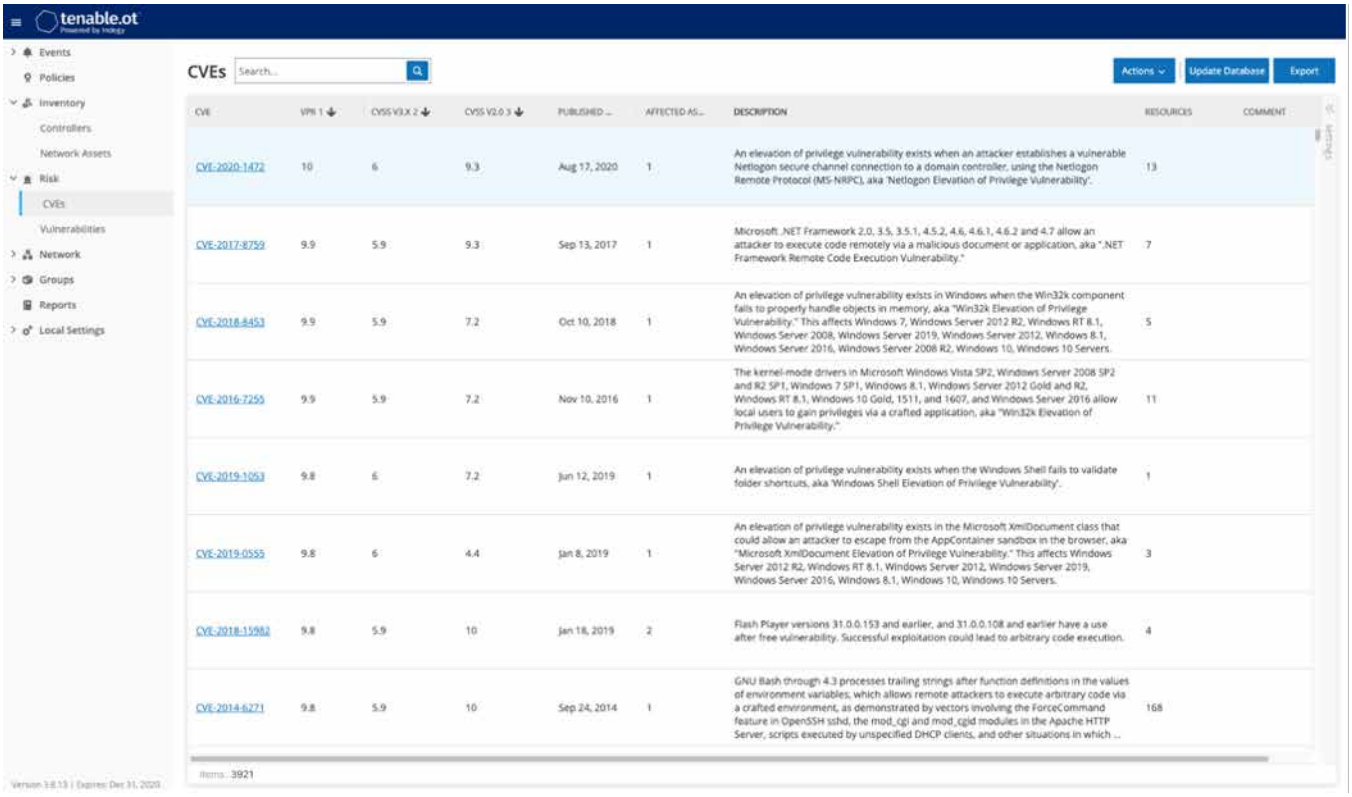
↓

Jede Schwachstelle erhält eine Prioritätsbewertung **auf einer Skala von 0 bis 10**.

→ Das Ergebnis: **97 % weniger** Schwachstellen, die umgehend Behebungsmaßnahmen erfordern.

ÜBER TENABLE.OT

Tenable.ot schützt industrielle und kritische Infrastrukturen vor Cyberbedrohungen, böswilligen Insidern und menschlichem Fehlverhalten. Von der Bedrohungserkennung und -eindämmung über Asset-Verfolgung und Schwachstellen-Management bis hin zu Konfigurationskontrolle und Prüfungen im Rahmen der adaptiven Bewertung – die Sicherheitsfunktionen für industrielle Steuerungssysteme (ICS) von Tenable maximieren die Sichtbarkeit, Sicherheit und Kontrolle in Ihren Betriebsumgebungen.



Weitere Informationen: Besuchen Sie de.tenable.com
Kontakt: Bitte senden Sie eine E-Mail an sales-de@tenable.com

COPYRIGHT 2021 TENABLE, INC. ALLE RECHTE VORBEHALTEN. TENABLE, TENABLE.IO, TENABLE NETWORK SECURITY, NESSUS, SECURITYCENTER, SECURITYCENTER CONTINUOUS VIEW UND LOG CORRELATION ENGINE SIND EINGETRAGENE MARKEN VON TENABLE, INC. TENABLE.SC, LUMIN, ASSURE UND THE CYBER EXPOSURE COMPANY SIND MARKEN VON TENABLE, INC. ALLE ANDEREN PRODUKTE BZW. SERVICES SIND MARKEN IHRER JEWEILIGEN INHABER.