

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 Angriffsfläche reduzieren, indem Sie bereits vor der NVD-Veröffentlichung Schwachstellen beseitigen, die aktiv ausgenutzt werden.

FUNKTIONSWEISE



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.

CVE	VPR 1	CVSS V3.X 2	CVSS V2.0 3	PUBLISHED	AFFECTED AS...	DESCRIPTION	RESOURCES	COMMENT
CVE-2020-1472	10	6	9.3	Aug 17, 2020	1	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability.'	13	
CVE-2017-8759	9.9	5.9	9.3	Sep 13, 2017	1	Microsoft .NET Framework 2.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 and 4.7 allow an attacker to execute code remotely via a malicious document or application, aka '.NET Framework Remote Code Execution Vulnerability.'	7	
CVE-2018-4453	9.9	5.9	7.2	Oct 10, 2018	1	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability.' This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers.	5	
CVE-2016-7255	9.9	5.9	7.2	Nov 10, 2016	1	The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka 'Win32k Elevation of Privilege Vulnerability.'	11	
CVE-2019-1053	9.8	6	7.2	Jun 12, 2019	1	An elevation of privilege vulnerability exists when the Windows Shell fails to validate folder shortcuts, aka 'Windows Shell Elevation of Privilege Vulnerability.'	1	
CVE-2019-0555	9.8	6	4.4	Jan 8, 2019	1	An elevation of privilege vulnerability exists in the Microsoft XmlDocument class that could allow an attacker to escape from the AppContainer sandbox in the browser, aka 'Microsoft XmlDocument Elevation of Privilege Vulnerability.' This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows Server 2019, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers.	3	
CVE-2018-15961	9.8	5.9	10	Jan 18, 2019	2	Flash Player versions 31.0.0.153 and earlier, and 31.0.0.108 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution.	4	
CVE-2014-6271	9.8	5.9	10	Sep 24, 2014	1	GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_log and mod_ssl modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which ...	168	

Items: 3921

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.