**MEDIENMITTEILUNG**

Zürich, 8. Juni 2022

**Brennpunkte sofort im Blick: WatchGuard launcht neue CVE-Übersichtsseite**

**Zentrale Anlaufstelle für Anwender sowie MSP- und Vertriebspartner von WatchGuard listet wichtige Informationen zu potenziellen Sicherheitslücken**

**Das Product Security Incident Response Team (PSIRT) von WatchGuard hat mit der neuen** [**CVE-Übersichtsseite**](https://www.watchguard.com/de/wgrd-psirt/advisories) **eine Plattform ins Leben gerufen, die sich speziell an alle Anwender sowie MSP- und Vertriebspartner von WatchGuard-Produkten richtet. Diese listet gegenwärtig bekannte Schwachstellen und Anfälligkeiten (Common Vulnerabilities and Exposures, CVE) im Einzelnen auf und bietet weiterführende Hinweise zum Umgang mit diesen Auffälligkeiten – über das gesamte WatchGuard-Portfolio hinweg. Darüber hinaus werden Einschätzungen und Untersuchungen zu branchenweiten Sicherheitsproblemen geteilt, die sich gegebenenfalls ebenso auf WatchGuard-Produkte oder -Services auswirken könnten. Netzwerkadministratoren und IT-Verantwortliche erhalten damit eine zentrale Anlaufstelle mit konsolidierten Informationen, die eine schnelle Reaktion auf aktuelle Sicherheitsereignisse ermöglichen. Alle Inhalte lassen sich zudem einfach und automatisiert via** [**RSS-Feed**](https://www.watchguard.com/de/wgrd-psirt/advisories.xml) **abrufen.**

Gleichzeitig finden White-Hat-Hacker und Sicherheitsforscher auf der Seite hilfreiche Informationen für den Fall, dass sie selbst eine – von ihnen identifizierte – Schwachstelle melden möchten. Neben einer konkreten [Anleitung](https://www.watchguard.com/de/wgrd-psirt/report-vulnerability), auf welche Informationen es im Zuge einer solchen Einreichung ankommt, ist ebenso eine [„Safe Harbor“-Klausel](https://www.watchguard.com/de/wgrd-psirt/responsible-disclosure-policy) aufgeführt. Mit dieser sichert WatchGuard den Schutz vor rechtlichen Schritten im Zusammenhang mit der Meldung und/oder Erforschung der Schwachstelle zu. Dazu Sven Wulf, Geschäftsführer der Schneider & Wulf EDV-Beratung GmbH & Co. KG: „Angesichts einer sich ständig ändernden Bedrohungssituation und insbesondere bei Zero-Day-Angriffen ist schnelles Handeln angesagt. Da bieten die von WatchGuard auf der neuen CVE-Übersichtseite proaktiv bereitgestellten Informationen sowie Handlungsempfehlungen einen unschätzbaren Vorteil im Kampf gegen Cybergefahren jeder Art.“

Ziel von WatchGuard ist es, Administratoren beim Erkennen wichtiger Sicherheitsprobleme zu unterstützen. Diese erhalten konkrete Hilfestellungen inklusive möglicher Workarounds. Auf der PSIRT-Seite werden Security Advisories aus den folgenden drei Hauptkategorien veröffentlicht:

* In die erste Kategorie fallen Schwachstellen, die das WatchGuard-Team selbst in den Firebox-Modelllinien sowie anderen Produkten identifiziert hat und die ein sofortiges Handeln erfordern. Es werden sowohl Details zur Schwachstelle und deren Schweregrad geteilt (ohne Informationen bereitzustellen, die für Angreifer nützlich sein könnten), als auch Hinweise zur Eindämmung bzw. konkrete Handlungsempfehlungen gegeben. Auf diese Weise können Administratoren die potenziellen Auswirkungen einer Schwachstelle schnell nachvollziehen und adäquat reagieren – beispielsweise über die konkret aufgeführten Software-Upgrades oder beschriebenen Konfigurationsänderungen.
* Des Weiteren finden branchenweit relevante Schwachstellen Berücksichtigung (ein Beispiel dafür ist [Log4Shell](https://www.secplicity.org/2021/12/10/critical-rce-vulnerability-in-log4js/)), deren potenzielle Auswirkungen auf eingesetzte WatchGuard-Produkte bei Kunden und Partnern Fragen aufwerfen. In dieser Kategorie versorgt WatchGuard Managed Services Provider und weitere Anwender mit allen relevanten Informationen, ohne dass sie diese aktiv anfordern oder an anderer Stelle danach suchen müssen.
* Zur dritten Kategorie gehören Hinweise zu Sicherheitslücken in WatchGuard-Produkten, die von externen Forschern gefunden wurden. Damit möchte WatchGuard die harte Arbeit all derjenigen wertschätzen, die im Rahmen eines offenen und verantwortungsvollen Dialogs mit dem Product Security Incident Response Team (PSIRT) zusammenarbeiten. Es geht darum, deren Arbeit bestmöglich zu würdigen und gleichzeitig Kunden ein umfassendes Bild von den von aussen aufgedeckten Schwachstellen und eventuellen Auswirkungen zu vermitteln.

**Sicherstellung der Compliance**

Die neue PSIRT-Seite vereinfacht Unternehmen nicht zuletzt die Einhaltung von Compliance-Richtlinien. Führen Administratoren Audits oder Schwachstellen-Scans durch, werden sie auf relevante CVEs und in dem Zusammenhang erforderliche Upgrades oder Korrekturen hingewiesen. Über die klare Gewichtung jeder einzelnen Schwachstelle entsprechend ihrem Schweregrads können IT-Administratoren und ihre Teams bei der Umsetzung von Gegenmassnahmen gezielt priorisieren. Kunden und Partner sollten jedoch grundsätzlich immer darauf achten, dass die WatchGuard-Produkte stets über die neueste Firmware verfügen und veröffentlichte Patches zeitnah installiert werden. Auf diese Weise können sie aktiv dazu beitragen, das Risiko so gering wie möglich zu halten.

Letztendlich spiegelt die PSIRT-Seite vor allem wider, wie viel Engagement WatchGuard aufbringt, damit Managed Service Provider, Partner und Kunden angesichts der zunehmend komplexer werdenden Bedrohungsszenarien den Angreifern stets den entscheidenden Schritt voraus bleiben können. Künftig werden im Zuge branchenweiter Best Practices sukzessive Informationen und Funktionen hinzukommen, um die Prozesse rund um die Verfolgung und Meldung von Schwachstellen weiter zu optimieren.

Bildmaterial

Das Bildmaterial zum Download finden Sie in unserem Medienportal press-n-relations.amid-pr.com (Suchbegriff „[WatchGuard PSIRT](https://press-n-relations.amid-pr.com/AMID-PR/searchresult/searchresult.xhtml?searchString=PSIRT&searchId=0&searchType=detailed)"). Selbstverständlich schicke ich Ihnen die Dateien auch gerne per E-Mail zu. Kontakt: rh@press-n-relations.de

|  |  |
| --- | --- |
|  |  |
| Sven Wulf, Geschäftsführer der Schneider & Wulf EDV-Beratung GmbH & Co. KG | Auf der neuen CVE-Übersichtsseite von WatchGuard werden bekannte Schwachstellen und Anfälligkeiten aufgelistet. |

|  |  |
| --- | --- |
| Kontakt:WatchGuard Technologies GmbHPaul Moll – Field Marketing Manager Central EuropeWendenstr. 379, 20537 HamburgTel.: +49 152 31795040paul.moll@watchguard.comhttps://www.watchguard.com/de | Presse- und Öffentlichkeitsarbeit:Press'n'Relations GmbHRebecca HornMagirusstr. 33, 89077 UlmTel.: +49 731 962 87 15 rh@press-n-relations.dehttps://press-n-relations.com |

**Über WatchGuard Technologies**

WatchGuard Technologies gehört zu den führenden Anbietern im Bereich IT-Sicherheit. Das umfangreiche Produktportfolio reicht von hochentwickelten UTM (Unified Threat Management)- und Next-Generation-Firewall-Plattformen über Multifaktor-Authen­tifizierung bis hin zu Technologien für umfassenden WLAN-Schutz und Endpoint Protection sowie weiteren spezifischen Produkten und intelligenten Services rund ums Thema IT-Security. Mehr als 250.000 Kunden weltweit vertrauen auf die ausgeklügelten Schutzmechanismen auf Enterprise-Niveau, wobei dank der einfachen Handhabung neben kleinen und mittelständischen Unternehmen nicht zuletzt auch grosse, dezentral aufgestellte Organisationen und Managed Services Provider vom Einsatz profitieren. Neben der Zentrale in Seattle im US-Bundesstaat Washington verfügt WatchGuard über Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum.

Aktuelle Informationen, Aktionen und Updates finden Sie auch auf [Twitter](https://twitter.com/sichersein), [Facebook](https://de-de.facebook.com/WatchGuardSichersein/) oder [LinkedIn](https://de.linkedin.com/company/watchguardsichersein). Der WatchGuard-Blog „Secplicity“ berichtet darüber hinaus über die neuesten Bedrohungen und zeigt auf, wie man mit ihnen umgeht: [www.secplicity.org](http://www.secplicity.org/). Oder Sie abonnieren den „443 – Security Simplified“-Podcast bei [Secplicity.org](http://www.secplicity.org/) bzw. wo immer Sie Ihre Lieblings-Podcasts finden.