Cybersecurity Morgenreport

Ausgabe: 20230804

Editorial

Guten Morgen,

willkommen zum Cybersecurity Morgenreport von Cyberwald, Ihrem täglichen Begleiter in der Welt der IT-Sicherheit. Als nicht-kommerzielles Projekt ist es unser Anliegen, Awareness und Wissen rund um das Thema Cybersecurity kostenlos zu vermitteln. In der heutigen digitalen Welt ist es für Unternehmen von entscheidender Bedeutung, sich über aktuelle Sicherheitsrisiken zeitnah zu informieren. Cyberbedrohungen entwickeln sich ständig weiter und können erhebliche Schäden verursachen, wenn sie nicht rechtzeitig erkannt und abgewehrt werden. Durch die Nutzung aktueller Informationen können Unternehmen ihre IT-Sicherheitsmaßnahmen stärken und sich effektiv gegen diese Bedrohungen schützen.

Unser Ziel ist es, Ihnen, den IT-Verantwortlichen, einen kompakten und leicht verständlichen Überblick über aktuelle Sicherheitsrisiken zu geben. Wir präsentieren Ihnen täglich Sicherheitsmeldungen und Berichte über neue Sicherheitslücken, die Ihre Systeme und Daten bedrohen könnten.

Darüber hinaus listen wir aktuelle Cyberangriffe und Ransomware-Vorfälle auf. Dies ist von besonderer Bedeutung, da es Unternehmen ermöglicht, sich auf mögliche Supply-Chain- und Phishing-Angriffe vorzubereiten. Durch das Verständnis der Methoden und Taktiken, die von Cyberkriminellen verwendet werden, können Unternehmen ihre Verteidigungsmaßnahmen entsprechend anpassen und stärken.

Für den Cybersecurity Morgenreport greifen wir automatisiert auf öffentliche Informationsquellen zu, filtern und sortieren diese Informationen, um sie Ihnen in einer übersichtlichen Form zur Verfügung zu stellen. Wir bemühen uns, die Inhalte so verständlich wie möglich zu gestalten und vorzugsweise vollständig in deutscher Sprache wiederzugeben. Bei Bedarf übersetzen wir die öffentlichen Informationen und fassen sie durch eine KI zusammen.

Der Cybersecurity Morgenreport ist ein dynamisches Projekt. Wir passen und erweitern unsere Inhalte ständig, um Ihnen die relevantesten und aktuellsten Informationen zu liefern. Derzeit befinden wir uns im Alpha-Stadium des Projekts und freuen uns über Ihr Feedback und Ihre Anregungen.

Wir hoffen, dass der Cybersecurity Morgenreport Ihnen hilft, Ihre IT-Sicherheitsmaßnahmen zu verbessern und Ihre Systeme vor den ständig wechselnden Bedrohungen zu schützen. Bleiben Sie sicher und informiert mit dem Cybersecurity Morgenreport von Cyberwald.

Ihr Cyberwald-Team

Security-News

Heise - Security-Alert

Sicherheitsupdates: Angreifer können Aruba-Switches kompromittieren
Bestimmte Switch-Modelle von Aruba sind verwundbar. Die Entwickler haben eine Sicherheitslücke geschlossen.
- Link

Upgrade nötig: Kritische Lücke bedroht ältere MobileIron-Ausgaben von Ivanti
Angreifer können an einer kritischen Schwachstelle in der nicht mehr im Support befindlichen Mobile-Device-Management-Lösung Ivanti MobileIron ansetzen.
- Link

Firefox, Thunderbird und Tor Browser bekommen Sicherheitsupdates
Angreifer könnten aus der Firefox-Sandbox ausbrechen. Die Entwickler haben noch weitere Lücken geschlossen.
- Link

Angreifer kapern Minecraft-Server über BleedingPipe-Exploit
Mehrere Mincecraft-Modifikationen weisen eine Schwachstelle auf, die Angreifer derzeit aktiv ausnutzen. Davon sollen neben Servern auch Clients betroffen sein.
- Link

Sicherheitsupdate: WordPress-Websites mit Plug-in Ninja Forms attackierbar
Angreifer könnten über eine Sicherheitslücke im Ninja-Forms-Plug-in auf eigentlich geschützte WordPress-Daten zugreifen.
- Link

Jetzt patchen! Ivanti schließt erneut Zero-Day-Lücke in EPMM
Derzeit nehmen Angreifer Ivanti Endpoint Manager Mobile (EPMM) ins Visier. Nun gibt es einen Patch gegen eine weitere Schwachstelle.
- Link

Angreifer können NAS- und IP-Videoüberwachungssysteme von Qnap lahmlegen
Mehrere Netzwerkprodukte von Qnap sind für eine DoS-Attacken anfällig. Dagegen abgesicherte Software schafft Abhilfe.
- Link

Jetzt patchen! Angreifer attackieren E-Mail-Lösung Zimbra
Es ist ein wichtiges Sicherheitsupdate für Zimbra Collaboration Suite erschienen. Admins sollten zügig handeln.
- Link

Sicherheitsupdate: Angreifer können Sicherheitslösung Sophos UTM attackieren
Sophos Unified Threat Management ist verwundbar. Aktuelle Software schafft Abhilfe.
- Link

Sicherheitsupdates: Angreifer können Access Points von Aruba übernehmen
Wenn die Netzwerkbetriebssysteme ArubaOS 10 oder InstantOS zum Einsatz kommen, sind Access Points von Aruba verwundbar.
- Link

Sicherheitslücken

Eine Sicherheitslücke oder Schwachstelle ist ein Fehler in einer Software oder Hardware, der es einem Angreifer ermöglicht, in ein Computersystem einzudringen und Schaden anzurichten. Diese Lücke stellt eine Bedrohung für die Sicherheit des Systems dar, da sie ausgenutzt werden kann, um das System zu kompromittieren. Sicherheitslücken entstehen oft durch unzureichenden Schutz des Computers vor Netzwerkangriffen, zum Beispiel durch fehlende Firewall oder andere Sicherheitssoftware. Auch Programmierfehler im Betriebssystem, Webbrowser oder anderen Anwendungen können Sicherheitslücken verursachen. Bekannte Sicherheitslücken sollten daher so schnell wie möglich durch das Einspielen eines Patches geschlossen werden, um die Angriffsfläche der IT-Systeme zu verringern.

EPSS

Das Exploit Prediction Scoring System wird für eine bekannte Software-Sicherheitslücke / CVE auf einer Skala von 0 (0%) bis 1 (100%) angegeben und soll die Wahrscheinlichkeit für das Auftreten eines Exploits in naher Zukunft darstellen. Ein höherer Wert bedeutet eine höhere Wahrscheinlichkeit, dass eine Schwachstelle in naher Zukunft ausgenutzt wird. EPSS kann auch als Rahmen für die Priorisierung von Schwachstellen unter Verwendung einer Kombination von Metriken betrachtet werden. Es soll Unternehmen dabei helfen, ihre Ressourcen effizienter zu verteilen und alle relevanten Cyber-Risiken zu minimieren.

CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34362	0.940540000	0.987880000	Link
CVE-2023-33246	0.955810000	0.991130000	Link
CVE-2023-28771	0.918810000	0.985100000	Link
CVE-2023-28121	0.937820000	0.987460000	Link
CVE-2023-27372	0.970730000	0.996490000	Link
CVE-2023-27350	0.971160000	0.996730000	Link
CVE-2023-25717	0.960700000	0.992480000	Link
CVE-2023-25194	0.918160000	0.985050000	Link
CVE-2023-21839	0.953670000	0.990560000	Link
CVE-2023-20887	0.960590000	0.992450000	Link
CVE-2023-0669	0.965030000	0.993870000	Link

BSI - Warn- und Informationsdienst (WID)

Thu, 03 Aug 2023
[UPDATE] [hoch] vim: Mehrere Schwachstellen ermöglichen Codeausführung
Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Code auszuführen, Speicher zu modifizieren und einen Denial of Service Zustand zu verursachen.
- Link

—

Thu, 03 Aug 2023
[UPDATE] [hoch] vim: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Programmcode auszuführen, einen Denial of Service Zustand herbeizuführen oder Dateien zu manipulieren.
- Link

—

Thu, 03 Aug 2023
[UPDATE] [hoch] vim: Mehrere Schwachstellen
Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in vim ausnutzen, um einen Denial of Service Angriff durchzuführen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen und den Speicher zu manipulieren.
- Link

—

Thu, 03 Aug 2023
[UPDATE] [hoch] vim: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und vertrauliche Informationen offenzulegen
- Link

—

Thu, 03 Aug 2023
[UPDATE] [hoch] Python: Schwachstelle ermöglicht Denial of Service
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Python ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

Thu, 03 Aug 2023
[UPDATE] [hoch] Red Hat OpenShift Container Platform: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der Red Hat OpenShift Container Platform ausnutzen, um Sicherheitsvorkehrungen zu umgehen.
- Link

—

Thu, 03 Aug 2023
[UPDATE] [hoch] Microsoft Developer Tools: Mehrere Schwachstellen
Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Microsoft .NET Framework, Microsoft Azure DevOps Server, Microsoft NuGet, Microsoft Visual Studio und Microsoft Visual Studio Code ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen, seine Rechte zu erweitern und Daten zu manipulieren.
- Link

—

Thu, 03 Aug 2023
[UPDATE] [hoch] Microsoft Developer Tools: Mehrere Schwachstellen
Ein entfernter, authentisierter oder anonymer Angreifer kann mehrere Schwachstellen in Microsoft Visual Studio 2022, Microsoft Visual Studio Code und Microsoft .NET Framework ausnutzen, um seine Privilegien zu erweitern, beliebigen Programmcode auszuführen, Sicherheitsvorkehrungen zu umgehen oder Dateien zu manipulieren.
- Link

—

Thu, 03 Aug 2023
[UPDATE] [hoch] OpenSSH: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in OpenSSH ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Thu, 03 Aug 2023
[NEU] [hoch] HP LaserJet: Schwachstelle ermöglicht Privilegieneskalation
Ein lokaler Angreifer kann eine Schwachstelle in HP LaserJet ausnutzen, um seine Privilegien zu erhöhen.
- Link

—

Thu, 03 Aug 2023
[UPDATE] [hoch] Ruby on Rails: Mehrere Schwachstellen
Ein entfernter Angreifer kann mehrere Schwachstellen in Ruby on Rails ausnutzen, um einen Denial of Service Angriff durchzuführen, Daten zu manipulieren und Sicherheitsmaßnahmen zu umgehen.
- Link

—

Thu, 03 Aug 2023
[UPDATE] [hoch] Linux Kernel (vmwgfx): Mehrere Schwachstellen
Ein lokaler Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um Informationen offenzulegen und um seine Privilegien zu erweitern.
- Link

—

Thu, 03 Aug 2023
[UPDATE] [hoch] Mozilla Firefox und Mozilla Thunderbird: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Programmcode auszuführen, seine Privilegien zu erweitern, Informationen offenzulegen, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen oder

Sicherheitsvorkehrungen zu umgehen.
- Link
—
Wed, 02 Aug 2023
[UPDATE] [hoch] Red Hat OpenShift (Logging Subsystem): Schwachstelle ermöglicht Denial of Service
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat OpenShift (Logging Subsystem) ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link
—
Wed, 02 Aug 2023
[UPDATE] [hoch] Grafana: Schwachstelle ermöglicht Übernahme von Benutzerkonto
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Grafana ausnutzen, um ein Benutzerkonto zu übernehmen.
- Link
—
Wed, 02 Aug 2023
[NEU] [hoch] Aruba Switch: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit Administratorrechten
Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Aruba Switch ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen.
- Link
—
Wed, 02 Aug 2023
[UPDATE] [hoch] Node.js: Mehrere Schwachstellen
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um seine Privilegien zu erweitern, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen, Informationen offenzulegen oder Sicherheitsvorkehrungen zu umgehen.
- Link
—
Wed, 02 Aug 2023
[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht nicht spezifizierten Angriff
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in QEMU ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.
- Link
—
Wed, 02 Aug 2023
[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen und potenziell, um Code auszuführen.
- Link
—
Wed, 02 Aug 2023
[UPDATE] [hoch] Red Hat OpenShift Container Platform: Schwachstelle ermöglicht Privilegieneskalation
Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Red Hat OpenShift Container Platform ausnutzen, um seine Privilegien zu erhöhen.
- Link
—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/3/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaFirefox (SUSE-SU-2023:3162-1)]	critical
8/3/2023	[SUSE SLES12 Security Update : MozillaFirefox (SUSE-SU-2023:3161-1)]	critical

Datum	Schwachstelle	Bewertung
8/3/2023	[Ivanti Endpoint Manager Mobile Remote Unauthenticated API Access (CVE-2023-35082)]	critical
8/3/2023	[Ivanti Endpoint Manager Mobile < 11.3 Remote Unauthenticated API Access (CVE-2023-35082)]	critical
8/3/2023	[Siemens Unauthenticated Access to Critical Services in SCALANCE X-200 Switch Family (CVE-2013-5944)]	critical
8/3/2023	[Siemens SCALANCE X-200RNA Switch Devices Use of Insufficiently Random Values (CVE-2022-46353)]	critical
8/3/2023	[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-6270-1)]	high
8/3/2023	[RHEL 8 : .NET 6.0 (RHSA-2023:4448)]	high
8/3/2023	[RHEL 9 : .NET 6.0 (RHSA-2023:4449)]	high
8/3/2023	[Debian DLA-3512-1 : linux-5.10 - LTS security update]	high
8/3/2023	[IBM DB2 DoS (7010561) (Unix)]	high
8/3/2023	[IBM DB2 DoS (7010561) (Windows)]	high
8/3/2023	[Red Hat Ansible Automation Platform 2.4 HTML Injection (RHSA-2023:4340)]	high
8/3/2023	[PHP 8.1.x < 8.1.22 Multiple Vulnerabilities]	high
8/3/2023	[CentOS 7 : kernel (CESA-2023:4151)]	high
8/3/2023	[CentOS 7 : bind (CESA-2023:4152)]	high
8/3/2023	[RHEL 8 : firefox (RHSA-2023:4464)]	high
8/3/2023	[RHEL 8 : firefox (RHSA-2023:4463)]	high
8/3/2023	[RHEL 9 : firefox (RHSA-2023:4465)]	high
8/3/2023	[RHEL 8 : firefox (RHSA-2023:4460)]	high
8/3/2023	[RHEL 7 : firefox (RHSA-2023:4461)]	high
8/3/2023	[RHEL 8 : firefox (RHSA-2023:4468)]	high
8/3/2023	[RHEL 8 : firefox (RHSA-2023:4469)]	high
8/3/2023	[RHEL 9 : firefox (RHSA-2023:4462)]	high
8/3/2023	[Oracle Linux 9 : kernel (ELSA-2023-4377)]	high
8/3/2023	[Ubuntu 16.04 ESM : XMLTooling vulnerability (USN-6274-1)]	high
8/3/2023	[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS : MaraDNS vulnerabilities (USN-6271-1)]	high
8/3/2023	[Ubuntu 16.04 ESM / 22.04 ESM : Cargo vulnerability (USN-6275-1)]	high
8/3/2023	[IBM DB2 Buffer Overflow (7010565) (Windows)]	high
8/3/2023	[IBM DB2 Buffer Overflow (7010565) (Unix)]	high
8/3/2023	[IBM DB2 Privilege Escalation (7010571) (Windows)]	high
8/3/2023	[PLC Cycle Time Influences Uncontrolled Resource Consumption (CVE-2019-10953)]	high
8/3/2023	[Siemens SCALANCE X-200RNA Switch Devices Exposure of Sensitive Information to an Unauthorized Actor (CVE-2022-46355)]	high
8/3/2023	[Siemens SCALANCE and RUGGEDCOM Products Missing Authorization (CVE-2022-31765)]	high
8/3/2023	[Siemens (CVE-2021-41990)]	high
8/3/2023	[Siemens SCALANCE X-200RNA Switch Devices Uncontrolled Resource Consumption (CVE-2022-46352)]	high

Die Hacks der Woche

mit Martin Haunschmid

Wasser predigen und Wein trinken? Ivanti, als Security Hersteller DARF so etwas nicht passieren!

Zum Youtube Video

Cyberangriffe: (Aug)

Datum	Opfer	Land	Information

Ransomware-Erpressungen: (Aug)

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-08-03	[Spokane Spinal Sports Care Clinic]	bianlian	Link
2023-08-03	[pointpleasant.k12.nj.us]	lockbit3	Link
2023-08-03	[Roman Catholic Diocese of Albany]	nokoyawa	Link
2023-08-03	[Venture General Agency]	akira	Link
2023-08-03	[Datawatch Systems]	akira	Link
2023-08-03	[admsc.com]	lockbit3	Link
2023-08-03	[United Tractors]	rhysida	Link
2023-08-03	[RevZero, Inc]	8base	Link
2023-08-03	[Rossman Realty Group, inc.]	8base	Link
2023-08-03	[riggsabney]	alphv	Link
2023-08-02	[fec-corp.com]	lockbit3	Link
2023-08-02	[bestmotel.de]	lockbit3	Link
2023-08-02	[Tempur Sealy International]	alphv	Link
2023-08-02	[constructioncrd.com]	lockbit3	Link
2023-08-02	[Helen F. Dalton Lawyers]	alphv	Link
2023-08-02	[TGRWA]	akira	Link
2023-08-02	[Guido]	akira	Link
2023-08-02	[Bickel & Brewer - Press Release]	monti	Link
2023-08-02	[SHERMAN.EDU]	clop	Link
2023-08-02	[COSI]	karakurt	Link
2023-08-02	[unicorpusa.com]	lockbit3	Link
2023-08-01	[Garage Living, The Dispenser USA]	play	Link
2023-08-01	[Aapd]	play	Link
2023-08-01	[Birch, Horton, Bittner & Cherot]	play	Link
2023-08-01	[DAL-TECH Engineering]	play	Link
2023-08-01	[Coral Resort]	play	Link
2023-08-01	[Professionnel France]	play	Link
2023-08-01	[ACTIVA Group]	play	Link
2023-08-01	[Aquatlantis]	play	Link
2023-08-01	[Kogetsu]	mallox	Link
2023-08-01	[Parathon by JDA eHealth Systems]	akira	Link
2023-08-01	[KIMCO Staffing Service]	alphv	Link
2023-08-01	[Pea River Electric Cooperative]	nokoyawa	Link
2023-08-01	[MBS Equipment TTI]	8base	Link
2023-08-01	[gerb.bg]	lockbit3	Link
2023-08-01	[persingerlaw.com]	lockbit3	Link
2023-08-01	[Jacklett Construction LLC]	8base	Link

Quellen

Quellenverzeichnis

1) Cyberwatch - https://github.com/Casualtek/Cyberwatch
2) Ransomware.live - https://data.ransomware.live
3) Heise Security Alerts! - https://www.heise.de/security/alerts/
4) First EPSS - https://www.first.org/epss/
5) BSI WID - https://wid.cert-bund.de/
6) Tenable Plugins - https://www.tenable.com/plugins/
7) Die Hacks der Woche - https://martinhaunschmid.com/videos

Impressum

Herausgeber:
Marlon Hübner
Brückenstraße 3
57629 Höchstenbach

E-Mail
info@cyberwald.com

Cyberwald ist ein privates, nicht-kommerzielles Projekt zur Förderung des Bewusstseins für Cybersicherheit.