Cybersecurity Morgenreport

Ausgabe: 20230802

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

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 erneute 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

—

Sicherheitsupdates: Sicherheitslücken bedrohen Hyperscale-Systeme von Lenovo
Angreifer könnten zwei Sicherheitslücken in Hyperscale-Systemen von Lenovo ausnutzen und Schadcode ausführen.
- Link

—

Jetzt patchen! Root-Sicherheitslücke gefährdet Mikrotik-Router
Stimmten die Voraussetzungen, können sich Angreifer in Routern von Mikrotik zum Super-Admin hochstufen.
- Link

—

Jetzt patchen! Weltweit über 15.000 Citrix-Server angreifbar
Sicherheitsforscher haben tausende verwundbare Citrix-Instanzen von Gateway und Netscaler ADC entdeckt. Davon sind auch Systeme in Deutschland betroffen.
- 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)

Tue, 01 Aug 2023
[NEU] [hoch] IBM Java: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in IBM Java ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Tue, 01 Aug 2023
[UPDATE] [hoch] OpenSSL: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in OpenSSL ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen, Sicherheitsvorkehrungen zu umgehen, Dateien zu manipulieren oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Tue, 01 Aug 2023
[UPDATE] [hoch] Red Hat OpenStack: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat OpenStack ausnutzen, um die Verfügbarkeit, Vertraulichkeit und Integrität zu gefährden.
- Link

—

Tue, 01 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

—

Tue, 01 Aug 2023
[UPDATE] [hoch] Zabbix: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Zabbix ausnutzen, um einen Denial of Service Angriff durchzuführen und um Informationen offenzulegen.
- Link

—

Mon, 31 Jul 2023
[NEU] [hoch] libarchive: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in libarchive ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Mon, 31 Jul 2023
[UPDATE] [hoch] QEMU: Mehrere Schwachstellen
Ein lokaler Angreifer kann mehrere Schwachstelle in QEMU ausnutzen, um einen Denial of Service Angriff durchzuführen und beliebigen Code auszuführen.
- Link

—

Mon, 31 Jul 2023
[UPDATE] [hoch] Apache Commons: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache Commons ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Mon, 31 Jul 2023
[UPDATE] [hoch] Apache Portable Runtime (APR): Mehrere Schwachstellen
Ein lokaler Angreifer kann mehrere Schwachstellen in Apache Portable Runtime (APR) ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Mon, 31 Jul 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

—

Mon, 31 Jul 2023
[UPDATE] [hoch] git: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in git ausnutzen, um Sicherheitsvorkehrungen zu umgehen, Daten zu manipulieren und seine Privilegien zu erweitern.
- Link

—

Mon, 31 Jul 2023
[UPDATE] [hoch] Ubuntu Linux: Mehrere Schwachstellen
Ein lokaler Angreifer kann mehrere Schwachstellen im Ubuntu Linux Kernel ausnutzen, um Sicherheitsvorkehrungen zu umgehen und seine Rechte zu erhöhen.
- Link

—

Fri, 28 Jul 2023
[NEU] [hoch] GStreamer: Mehrere Schwachstellen ermöglichen Codeausführung
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in GStreamer ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Fri, 28 Jul 2023
[NEU] [hoch] libsndfile: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in libsndfile ausnutzen, um beliebigen Code auszuführen, einen 'Denial of Service'-Zustand herbeizuführen oder einen nicht spezifizierten Angriff durchzuführen.
- Link

—

Fri, 28 Jul 2023

[UPDATE] [kritisch] TCP/IP Stack: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in TCP/IP Stack ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, einen Denial of Service Angriff durchzuführen, vertrauliche Daten einzusehen oder Daten zu manipulieren.
- Link

—

Fri, 28 Jul 2023

[UPDATE] [hoch] VMware Tanzu Spring Framework: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in VMware Tanzu Spring Framework ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Fri, 28 Jul 2023

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen, beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Fri, 28 Jul 2023

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit Administratorrechten

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen.
- Link

—

Fri, 28 Jul 2023

[UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen und seine Privilegien zu erweitern.
- Link

—

Fri, 28 Jul 2023

[UPDATE] [hoch] Apple iOS: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, vertrauliche Kernel-Zustände zu verändern, seine Privilegien zu erhöhen, einen Denial-of-Service zu verursachen oder Sicherheitsmaßnahmen zu umgehen. Eine erfolgreiche Ausnutzung erfordert eine Benutzerinteraktion.
- Link

—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/1/2023	[Mozilla Firefox ESR < 115.1]	critical
8/1/2023	[Mozilla Firefox ESR < 115.1]	critical
8/1/2023	[Mozilla Firefox < 116.0]	critical
8/1/2023	[Mozilla Firefox < 116.0]	critical
8/1/2023	[Mozilla Firefox ESR < 102.14]	critical
8/1/2023	[Mozilla Firefox ESR < 102.14]	critical
8/1/2023	[RHEL 8 : openssh (RHSA-2023:4384)]	critical

Datum	Schwachstelle	Bewertung
8/1/2023	[RHEL 8 : openssh (RHSA-2023:4383)]	critical
8/1/2023	[RHEL 7 : openssh (RHSA-2023:4382)]	critical
8/1/2023	[RHEL 8 : openssh (RHSA-2023:4381)]	critical
8/1/2023	[RHEL 9 : openssh (RHSA-2023:4412)]	critical
8/1/2023	[Ivanti Endpoint Manager Mobile Remote Unauthenticated API Access (CVE-2023-35078)]	critical
8/1/2023	[RHEL 8 : openssh (RHSA-2023:4419)]	critical
8/1/2023	[RHEL 8 : openssh (RHSA-2023:4413)]	critical
8/1/2023	[IBM Java 7.1 < 7.1.5.19 / 8.0 < 8.0.8.5]	high
8/1/2023	[Citrix Secure Access < 23.5.1.3 Privilege Escalation (CTX561480)]	high
8/1/2023	[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : librsvg vulnerability (USN-6266-1)]	high
8/1/2023	[RHEL 9 : kpatch-patch (RHSA-2023:4380)]	high
8/1/2023	[RHEL 8 : mod_auth_openidc:2.3 (RHSA-2023:4408)]	high
8/1/2023	[RHEL 9 : cjose (RHSA-2023:4411)]	high
8/1/2023	[RHEL 9 : kernel-rt (RHSA-2023:4378)]	high
8/1/2023	[RHEL 8 : mod_auth_openidc:2.3 (RHSA-2023:4409)]	high
8/1/2023	[RHEL 8 : mod_auth_openidc:2.3 (RHSA-2023:4410)]	high
8/1/2023	[RHEL 9 : kernel (RHSA-2023:4377)]	high
8/1/2023	[Samba 4.16.x < 4.16.10 / 4.17.x < 4.17.9 / 4.18.x < 4.18.4 Multiple Vulnerabilities]	high
8/1/2023	[GitLab 9.3 < 16.0.8 / 16.1 < 16.1.3 / 16.2 < 16.2.2 (CVE-2023-3994)]	high
8/1/2023	[GitLab 8.14 < 16.0.8 / 16.1 < 16.1.3 / 16.2 < 16.2.2 (CVE-2023-3364)]	high
8/1/2023	[RHEL 9 : cjose (RHSA-2023:4417)]	high
8/1/2023	[RHEL 8 : mod_auth_openidc:2.3 (RHSA-2023:4418)]	high
8/1/2023	[CentOS 8 : mod_auth_openidc:2.3 (CESA-2023:4418)]	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
2023-08-01	[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.