Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250207

Inhaltsverzeichnis

1 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

2 Security-News

2.1 Heise - Security-Alert

Cisco stopft Sicherheitslücken in mehreren Produkten – auch kritische

In mehreren Produkten hat Cisco Sicherheitslücken entdeckt und warnt in Sicherheitsmitteilungen davor. Updates stehen bereit.

- Link

—

Quartalssicherheitsupdates: F5 rüstet BIG-IP-Appliances gegen mögliche Angriffe

Die F5-Entwickler haben mehrere Sicherheitslücken in unter anderem BIG-IP Next und BIG-IQ geschlossen. Es kann zur Ausführung von Schadcode kommen.

- Link

—

CISA warnt vor Angriffen auf Linux, Apache OFBiz, .NET und Paessler PRTG

DIe US-amerikanische Cybersicherheitsbehörde CISA warnt vor beobachteten Angriffen auf Lücken in Linux, Apache OFBiz, .NET und Paessler PRTG.

- Link

—

HP: Kritische Lücken in Universal-Druckertreiber ermöglichen Codeschmuggel

HP hat die Universal-Druckertreiber für PCL 6 und Postscript aktualisiert. Die Updates schließen kritische Sicherheitslücken.

- Link

—

Netgear: Nighthawk Pro Gaming-Router mit Schadcode-Leck

Netgear warnt vor Codeschmuggel-Lücken in Nighthawk Pro Gaming-Routern. Zudem haben einige Router nach Support-Ende eine Sicherheitslücke.

- Link

—

Veeam Backup: Codeschmuggel durch MitM-Lücke im Updater möglich

Veeam Backup enthält einen Updater, der für Man-in-the-Middle-Attacken anfällig ist. Angreifer können Schadcode einschleusen.

- Link

—

Zugriffsmanagement: HPE Aruba Networking CPPM ist verwundbar

Netzwerkadmins sollten HPE Aruba Networking ClearPass Policy Manager aus Sicherheitsgründen aktualisieren.

- Link

—

Support ausgelaufen: Keine Sicherheitsupdates mehr für attackierte Zyxel-Router

Derzeit hat es eine Mirai-Botnet-Malware auf bestimmte Routermodelle von Zyxel abgesehen. Weil der Support ausgelaufen ist, müssen Admins jetzt handeln.

- Link

—

Patchday Android: Angreifer nutzen Kernel-Sicherheitslücke aus

Es sind wichtige Sicherheitsupdates für Android 12, 12L, 13, 14 und 15 erschienen. Angreifer können Geräte kompromittieren.

- Link

—

HP Anyware: Linux-Client ermöglicht Rechteausweitung

In HPs Anyware-Client für Linux können Angreifer ihre Rechte am System ausweiten. Ein Softwareupdate steht bereit, das den Fehler korrigiert.

- Link

—

3 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.

3.1 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.

3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-9474	0.974800000	0.999850000	Link
CVE-2024-9465	0.943220000	0.994120000	Link
CVE-2024-9463	0.961860000	0.996670000	Link
CVE-2024-8963	0.967240000	0.997830000	Link
CVE-2024-7593	0.971650000	0.999000000	Link
CVE-2024-6893	0.938390000	0.993650000	Link
CVE-2024-6670	0.910490000	0.991400000	Link
CVE-2024-5910	0.962890000	0.996900000	Link
CVE-2024-55956	0.967520000	0.997890000	Link
CVE-2024-5217	0.933860000	0.993170000	Link
CVE-2024-50623	0.969230000	0.998340000	Link
CVE-2024-4879	0.934670000	0.993250000	Link
CVE-2024-4577	0.958420000	0.996110000	Link
CVE-2024-4358	0.925270000	0.992460000	Link
CVE-2024-41713	0.957210000	0.995900000	Link
CVE-2024-40711	0.963400000	0.997000000	Link
CVE-2024-4040	0.969020000	0.998280000	Link
CVE-2024-38856	0.942880000	0.994100000	Link
CVE-2024-36401	0.952840000	0.995230000	Link
CVE-2024-3400	0.964000000	0.997110000	Link
CVE-2024-3273	0.937410000	0.993540000	Link
CVE-2024-32113	0.914790000	0.991680000	Link
CVE-2024-28995	0.965000000	0.997310000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-28987	0.961930000	0.996680000	Link
CVE-2024-27348	0.960260000	0.996400000	Link
CVE-2024-27198	0.968000000	0.998020000	Link
CVE-2024-24919	0.959630000	0.996280000	Link
CVE-2024-23897	0.973540000	0.999550000	Link
CVE-2024-23692	0.964470000	0.997220000	Link
CVE-2024-21893	0.956970000	0.995840000	Link
CVE-2024-21887	0.973220000	0.999480000	Link
CVE-2024-20767	0.965330000	0.997390000	Link
CVE-2024-1709	0.957220000	0.995900000	Link
CVE-2024-1212	0.937140000	0.993510000	Link
CVE-2024-0986	0.955530000	0.995660000	Link
CVE-2024-0195	0.962680000	0.996850000	Link
CVE-2024-0012	0.969980000	0.998530000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Thu, 06 Feb 2025

[NEU] [hoch] Cisco IOS, IOS XE and IOS XR: Mehrere Schwachstellen ermöglichen Denial of Service

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Cisco IOS, Cisco IOS XE und Cisco IOS XR ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Thu, 06 Feb 2025

[NEU] [kritisch] F5 BIG-IP: Mehrere Schwachstellen

Ein Angreifer kann diese Schwachstellen ausnutzen, um beliebige Systembefehle auszuführen, Sicherheitsmaßnahmen zu umgehen, Cross-Site-Scripting-Angriffe durchzuführen und einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Thu, 06 Feb 2025

[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Oracle MySQL ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- Link

—

Thu, 06 Feb 2025

[UPDATE] [hoch] Mozilla Firefox und Thunderbird: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen preiszugeben, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu erzeugen oder Spoofing-Angriffe durchzuführen.

- Link

—

Thu, 06 Feb 2025

[NEU] [hoch] Apache Camel for Spring Boot: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Apache Camel, Red Hat Enterprise Linux und Red Hat Integration ausnutzen, um beliebigen Code auszuführen und Sicherheitsmaßnahmen zu umgehen.

- Link

—

Thu, 06 Feb 2025

[NEU] [hoch] Golang Go: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um Informationen offenzulegen, oder Code auszuführen.

- Link

—

Thu, 06 Feb 2025

[NEU] [hoch] Kemp LoadMaster: Mehrere Schwachstellen

Ein Angreifer aus einem angrenzenden Netzwerk kann mehrere Schwachstellen in Kemp LoadMaster ausnutzen, um beliebigen Programmcode auszuführen oder Informationen offenzulegen.

- Link

—

Thu, 06 Feb 2025

[NEU] [hoch] Red Hat Enterprise Linux (Fast Datapath): Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Thu, 06 Feb 2025

[NEU] [hoch] Cisco Identity Services Engine (ISE): Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in der Cisco Identity Services Engine (ISE) ausnutzen, um beliebigen Code mit Administratorrechten auszuführen, Sicherheitsmaßnahmen zu umgehen und Cross-Site-Scripting-Angriffe durchzuführen.

- Link

—

Thu, 06 Feb 2025

[NEU] [UNGEPATCHT] [hoch] Asterisk: Schwachstelle ermöglicht Codeausführung

Ein entfernter Angreifer kann eine Schwachstelle in Asterisk ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 06 Feb 2025

[UPDATE] [hoch] Apple iOS und Apple iPadOS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS ausnutzen, um vertrauliche Informationen offenzulegen, einen Phishing-Angriff durchzuführen, seine Privilegien zu erweitern, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen oder beliebigen Code auszuführen.

- Link

—

Thu, 06 Feb 2025

[UPDATE] [hoch] Apple Safari: Mehrere Schwachstellen

Ein anonymer Angreifer kann mehrere Schwachstellen in Apple Safari ausnutzen, um Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen oder vertrauliche Informationen offenzulegen.

- Link

—

Thu, 06 Feb 2025

[UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand herbeizuführen, Spoofing-Angriffe durchzuführen, Daten zu ändern, Sicherheitsmaßnahmen zu umgehen und vertrauliche Informationen offenzulegen

- Link

—

Thu, 06 Feb 2025

[UPDATE] [hoch] bzip2: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit den Rechten des Dienstes

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in bzip2 ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen.

- Link

—

Thu, 06 Feb 2025

[UPDATE] [hoch] PostgreSQL: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen und um Informationen offenzulegen.

- Link

—

Thu, 06 Feb 2025

[UPDATE] [hoch] Red Hat Satellite: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat Satellite ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Thu, 06 Feb 2025

[UPDATE] [hoch] PostgreSQL: Mehrere Schwachstellen

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um Informationen offenzulegen, beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Thu, 06 Feb 2025

[UPDATE] [hoch] less: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in less ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 06 Feb 2025

[UPDATE] [hoch] Red Hat OpenShift: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um Dateien zu manipulieren, einen Denial-of-Service-Zustand zu verursachen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, seine Privilegien zu erweitern oder um weitere nicht spezifizierte

Angriffe auszuführen.
- Link
—
Thu, 06 Feb 2025
[UPDATE] [hoch] Red Hat OpenShift Service Mesh Containers: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in Red Hat OpenShift Service Mesh Containers ausnutzen, um Dateien zu manipulieren, einen 'Denial of Service'-Zustand erzuegen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder weitere nicht spezifizierte Angriffe durchzuführen.
- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
2/6/2025	[Oracle Linux 7 : raptor2 (ELSA-2025-0319)]	critical
2/5/2025	[Amazon Linux 2023 : amazon-ssm-agent (ALAS2023-2025-824)]	critical
2/5/2025	[Amazon Linux 2023 : runfinch-finch (ALAS2023-2025-834)]	critical
2/5/2025	[Amazon Linux 2023 : containerd, containerd-stress (ALAS2023-2025-835)]	critical
2/5/2025	[Amazon Linux 2023 : nerdctl (ALAS2023-2025-833)]	critical
2/5/2025	[Amazon Linux 2023 : python3-virtualenv (ALAS2023-2025-831)]	critical
2/5/2025	[Slackware Linux 15.0 / current curl Multiple Vulnerabilities (SSA:2025-036-01)]	critical
2/5/2025	[Slackware Linux 15.0 / current mozilla-thunderbird Multiple Vulnerabilities (SSA:2025-036-03)]	critical
2/6/2025	[Debian dsa-5859 : chromium - security update]	high
2/6/2025	[Fedora 41 : java-latest-openjdk (2025-f27fcf5da3)]	high
2/6/2025	[Fedora 41 : java-1.8.0-openjdk (2025-dd11f92771)]	high

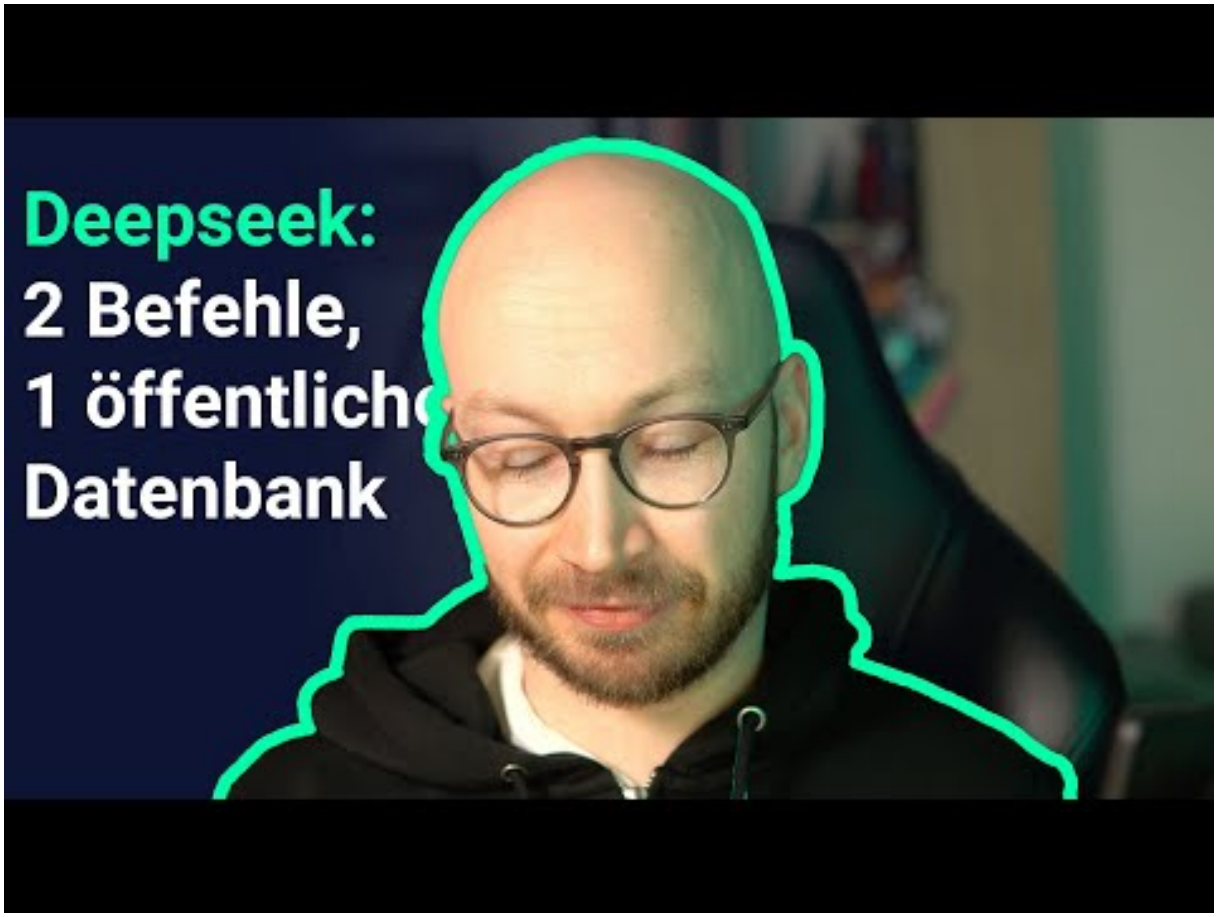
Datum	Schwachstelle	Bewertung
2/6/2025	[Fedora 41 : java-17-openjdk (2025-22db9134a2)]	high
2/6/2025	[Fedora 41 : java-11-openjdk (2025-e6f20785e3)]	high
2/6/2025	[Fedora 41 : FlightGear / SimGear (2025-b3322818a5)]	high
2/6/2025	[Aruba ClearPass Policy Manager 6.11.x < 6.11.10 / 6.12.x < 6.12.4 Multiple Vulnerabilities]	high
2/6/2025	[PDF-XChange Editor < 10.4.2.390 Multiple Vulnerabilities]	high
2/6/2025	[PDF-XChange Editor < 10.4.1.389 Multiple Vulnerabilities]	high
2/6/2025	[Atlassian Confluence 3.x < 7.19.29 / 8.0.x < 8.5.17 / 8.6.x < 8.9.8 / 9.0.1 < 9.1.1 (CONFSERVER-98484)]	high
2/6/2025	[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GNU C Library vulnerability (USN-7259-1)]	high
2/6/2025	[Atlassian Confluence 3.x < 7.19.30 / 7.20.x < 8.5.18 / 8.6.x < 9.1.1 / 9.2.0 (CONFSERVER-98842)]	high
2/6/2025	[Atlassian Jira Service Management Data Center and Server 5.12.x < 5.12.15 / 5.17.x < 5.17.5 / 10.3.x < 10.3.1 (JSDSERVER-15988)]	high
2/6/2025	[VMware Aria Operations Information Disclosure (VMSA-2025-0003)]	high
2/6/2025	[Amazon DCV Client <= 2023.1.8993 MITM]	high
2/6/2025	[Amazon DCV Client <= 2023.1.6203 MITM]	high
2/6/2025	[Microsoft Edge (Chromium) < 133.0.3065.51 Multiple Vulnerabilities]	high
2/5/2025	[Amazon Linux AMI : less (ALAS-2025-1958)]	high
2/5/2025	[Amazon Linux AMI : postgresql92 (ALAS-2025-1959)]	high
2/5/2025	[Amazon Linux 2023 : python3.11, python3.11-devel, python3.11-idle (ALAS2023-2025-829)]	high
2/5/2025	[Amazon Linux 2023 : nodejs20, nodejs20-devel, nodejs20-full-i18n (ALAS2023-2025-822)]	high
2/5/2025	[Amazon Linux 2023 : bpftool, kernel, kernel-devel (ALAS2023-2025-823)]	high

Datum	Schwachstelle	Bewertung
2/5/2025	[Amazon Linux 2023 : wireshark-cli, wireshark-devel (ALAS2023-2025-837)]	high
2/5/2025	[Amazon Linux 2023 : bpftool, kernel, kernel-devel (ALAS2023-2025-836)]	high
2/5/2025	[Amazon Linux 2023 : bind, bind-chroot, bind-devel (ALAS2023-2025-838)]	high
2/5/2025	[Amazon Linux AMI : kernel (ALAS-2025-1957)]	high
2/5/2025	[Schneider Electric EcoStruxure Control Expert, EcoStruxure Process Expert, and Modicon M340, M580 and M580 Safety PLCs Improper Enforcement of Message Integrity During Transmission in a Communication Channel (CVE-2023-6408)]	high

4 Die Hacks der Woche

mit Martin Haunschmid

4.0.1 Wo gehyped wird fallen Späne. Öffentliche Datenbank bei Deepseek



Zum Youtube Video

5 Cyberangriffe: (Feb)

Datum	Opfer	Land	Information
2025-02-05	IMI	[GBR]	Link
2025-02-02	Top-Medien	[CHE]	Link
2025-02-02	Mayer Steel Pipe Corporation	[TWN]	Link
2025-02-02	Nan Ya PCB (KunShan) Corp.	[TWN]	Link
2025-02-01	CESI	[FRA]	Link

6 Ransomware-Erpressungen: (Feb)

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-02-06	[harcoboe.net]	safepay	Link
2025-02-06	[lowernazareth.com]	safepay	Link
2025-02-06	[northernresponse.com]	cactus	Link
2025-02-06	[savoiesfoods.com]	cactus	Link
2025-02-06	[zsattorneys.com]	ransomhub	Link
2025-02-06	[NG-BLU Networks]	akira	Link
2025-02-06	[Presence From Innovation (PFI)]	akira	Link
2025-02-06	[Robertshaw]	hunters	Link
2025-02-05	[HARADA]	qilin	Link
2025-02-06	[DIEM]	fog	Link
2025-02-06	[Top Systems]	fog	Link
2025-02-06	[eConceptions]	fog	Link
2025-02-06	[Gitlabs: eConceptions, Top Systems, DIEM]	fog	Link
2025-02-05	[McCORMICK TAYLOR]	qilin	Link
2025-02-05	[www.iecsolutions.com]	safepay	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-02-05	[corehandf.com]	threeam	Link
2025-02-05	[Dash Business]	bianlian	Link
2025-02-05	[Hall Chadwick]	bianlian	Link
2025-02-05	[NESCTC Security Services]	bianlian	Link
2025-02-05	[Shinsung Delta Tech]	lynx	Link
2025-02-05	[Banfi Vintners]	lynx	Link
2025-02-05	[annegrady.org]	ransomhub	Link
2025-02-05	[rablighting.com]	qilin	Link
2025-02-05	[boostheat.com]	apt73	Link
2025-02-05	[rattelacademy.com]	funksec	Link
2025-02-05	[cara.com.my]	funksec	Link
2025-02-05	[Mid-State Machine & Fabricating Corp]	play	Link
2025-02-04	[casperstruck.com]	kairos	Link
2025-02-04	[medicalreportsltd.com]	kairos	Link
2025-02-01	[LUA Coffee]	fog	Link
2025-02-01	[GFZ Helmholtz Centre for Geosciences]	fog	Link
2025-02-01	[PT. ITPRENEUR INDONESIA TECHNOLOGY]	fog	Link
2025-02-04	[Devlion]	fog	Link
2025-02-04	[SOLEIL]	fog	Link
2025-02-04	[hemio.de]	fog	Link
2025-02-03	[Madia]	fog	Link
2025-02-03	[X-lab group]	fog	Link
2025-02-03	[Bolin Centre for Climate Research]	fog	Link
2025-02-04	[Gitlabs: hemio.de, SOLEIL, Devlion]	fog	Link
2025-02-04	[escada.com]	ransomhub	Link
2025-02-04	[mielectric.com.br]	akira	Link
2025-02-04	[engineeredequip.com]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-02-04	[emin.cl]	akira	Link
2025-02-04	[alphascriptrx.com]	akira	Link
2025-02-04	[premierop.com]	akira	Link
2025-02-04	[acesaz.com]	akira	Link
2025-02-04	[mipa.com.br]	akira	Link
2025-02-04	[usm-americas.com]	akira	Link
2025-02-04	[feheq.com]	akira	Link
2025-02-04	[stewartautosales.com]	akira	Link
2025-02-04	[milleraa.com]	akira	Link
2025-02-04	[jsfrental.com]	akira	Link
2025-02-04	[summitmovinghouston.com]	akira	Link
2025-02-04	[dwgp.com]	akira	Link
2025-02-04	[easycom.com]	akira	Link
2025-02-04	[alfa.com.co]	akira	Link
2025-02-04	[westernwoodsinc.com]	akira	Link
2025-02-04	[viscira.com]	akira	Link
2025-02-04	[elitt-sas.fr]	akira	Link
2025-02-04	[cfctech.com]	akira	Link
2025-02-04	[armellini.com]	akira	Link
2025-02-04	[mbacomputer.com]	akira	Link
2025-02-04	[directex.net]	akira	Link
2025-02-04	[360energy.com.ar]	akira	Link
2025-02-04	[saludsa.com.ec]	akira	Link
2025-02-04	[intercomp.com.mt]	akira	Link
2025-02-04	[sportadmin.se]	ransomhub	Link
2025-02-04	[C & R Molds Inc]	bianlian	Link
2025-02-04	[Commercial Solutions]	bianlian	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-02-04	[www.aymcdonald.com]	ransomhub	Link
2025-02-04	[capstoneins.ca]	ransomhub	Link
2025-02-04	[clarkfreightways.com]	ransomhub	Link
2025-02-04	[mistralsolutions.com]	apt73	Link
2025-02-04	[India car owners]	apt73	Link
2025-02-04	[AIshu, Eshoo]	ransomhouse	Link
2025-02-04	[kksp.com]	qilin	Link
2025-02-04	[brainsystem.eu]	funksec	Link
2025-02-04	[Taking stock of 2024	Part 2]	akira
2025-02-04	[esle.eu]	funksec	Link
2025-02-04	[forum-rainbow-rp.forumotion.eu]	funksec	Link
2025-02-04	[mgainnovation.com]	cactus	Link
2025-02-04	[cornwelltools.com]	cactus	Link
2025-02-04	[rashtiandrashti.com]	cactus	Link
2025-02-04	[alojaimi.com]	ransomhub	Link
2025-02-04	[www.aswgr.com]	ransomhub	Link
2025-02-04	[heartlandrvs.com]	ransomhub	Link
2025-02-04	[gaheritagefcu.org]	ransomhub	Link
2025-02-04	[SSMC]	cicada3301	Link
2025-02-04	[Rivers Casino and Rush Street Gaming]	cicada3301	Link
2025-02-04	[Asterra Properties]	cicada3301	Link
2025-02-04	[Caliente Construction]	cicada3301	Link
2025-02-04	[C2S Technologies Inc.]	everest	Link
2025-02-04	[ITSS]	everest	Link
2025-02-03	[brewsterfiredepartment.org]	safepay	Link
2025-02-03	[Dickerson & Nieman Realtors]	play	Link
2025-02-03	[Sheridan Nurseries]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-02-03	[The Hill Brush]	play	Link
2025-02-03	[DPC Development]	play	Link
2025-02-03	[Woodway USA]	play	Link
2025-02-03	[Daniel Island Club]	play	Link
2025-02-03	[QGS Development]	play	Link
2025-02-03	[Gitlabs: Bolin Centre for Climate Research, X-lab group, Madia]	fog	Link
2025-02-03	[gruppozaccaria.it]	lockbit3	Link
2025-02-03	[Karadeniz Holding (karadenizholding.com)]	fog	Link
2025-02-03	[www.wongfleming.com]	ransomhub	Link
2025-02-03	[smithmidland.com]	ransomhub	Link
2025-02-03	[www.origene.com]	ransomhub	Link
2025-02-03	[Denton Regional Suicide Prevention Coalition]	qilin	Link
2025-02-03	[fasttrackcargo.com]	funksec	Link
2025-02-03	[Ponte16 Hotel & Casino]	killsec	Link
2025-02-03	[Elslaw.com (EARLY , LUCARELLI , SWEENEY & MEISENKOTHEN LAW)]	qilin	Link
2025-02-03	[DRI Title & Escrow]	qilin	Link
2025-02-03	[DPA Auctions]	qilin	Link
2025-02-03	[Altair Travel]	qilin	Link
2025-02-03	[Civil Design, Inc]	qilin	Link
2025-02-03	[The Gatesworth Senior Living St. Louis]	qilin	Link
2025-02-03	[GOVirtual-it.com (VIRTUAL IT)]	qilin	Link
2025-02-03	[coel.com.mx]	apt73	Link
2025-02-03	[Alford Walden Law]	qilin	Link
2025-02-03	[Pasco Systems]	qilin	Link
2025-02-03	[MPP Group of Companies]	qilin	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-02-03	[Pineland community service board]	spacebears	Link
2025-02-02	[usuhs.edu]	lockbit3	Link
2025-02-02	[Four Eye Clinics]	abyss	Link
2025-02-02	[jpcgroupinc.com]	abyss	Link
2025-02-02	[hreu.eu]	funksec	Link
2025-02-02	[Tosaf]	handala	Link
2025-02-02	[turbomp]	stormous	Link
2025-02-02	[Cyrious Software]	bianlian	Link
2025-02-02	[Medical Associates of Brevard]	bianlian	Link
2025-02-02	[Civic Committee]	bianlian	Link
2025-02-02	[Ayres Law Firm]	bianlian	Link
2025-02-02	[Growth Acceleration Partners]	bianlian	Link
2025-02-01	[fiberskynet.net]	funksec	Link
2025-02-01	[tirtaraharja.co.id]	funksec	Link
2025-02-01	[Gitlabs: PT. ITPRENEUR INDONESIA TECHNOLOGY, GFZ Helmholtz Centre for Geosciences, LUA Cof…]	fog	Link
2025-02-01	[myisp.live]	funksec	Link
2025-02-01	[DATACONSULTANTS.COM]	clop	Link
2025-02-01	[CHAMPIONHOMES.COM]	clop	Link
2025-02-01	[CIERANT.COM]	clop	Link
2025-02-01	[DATATRAC.COM]	clop	Link
2025-02-01	[Nano Health]	killsec	Link
2025-02-01	[St. Nicholas School]	8base	Link
2025-02-01	[Héron]	8base	Link
2025-02-01	[Tan Teck Seng Electric (Co) Pte Ltd]	8base	Link
2025-02-01	[High Learn Ltd]	8base	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-02-01	[CAMRIDGEPORT]	spacebears	Link
2025-02-01	[Falcon Gaming]	arcusmedia	Link
2025-02-01	[Eascon]	arcusmedia	Link
2025-02-01	[Utilissimo Transportes]	arcusmedia	Link
2025-02-01	[GATTELLI SpA]	arcusmedia	Link
2025-02-01	[Technico]	arcusmedia	Link
2025-02-01	[Wireless Solutions (Morris.Domain)]	lynx	Link

7 Quellen

7.1 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) Exploit - packetstormsecurity.com
8) 0-Day - https://www.zerodayinitiative.com/rss/published/
9) Die Hacks der Woche - https://martinhaunschmid.com/videos

8 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.