Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240117

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

Kritische Sicherheitslücke: VMware vergaß Zugriffskontrollen in Aria Automation

Angreifer mit einem gültigen Konto können sich erweiterte Rechte verschaffen. VMWare bietet Patches an, Cloud-Kunden bleiben verschont.

- Link

—

Atlassian: Updates zum Patchday schließen 28 hochriskante Schwachstellen

Atlassian veranstaltet einen Patchday und schließt dabei 28 Sicherheitslücken in diversen Programmen, die als hohes Risiko gelten.

- Link

—

Cross-Site-Scripting in Monitoringsoftware PRTG erlaubt Sessionklau

Mit einem präparierten Link können Angreifer PRTG-Nutzer in die Irre führen und die Authentifizierung umgehen. Ein Update schafft Abhilfe.

- Link

—

Nvidia-Updates schließen kritische Sicherheitslücken in KI-Systemen

Nvidia hat aktualisierte Firmware für die KI-Systeme DGX A100 und H100 veröffentlicht. Sie dichtet kritische Sicherheitslecks ab.

- Link

—

Jetzt patchen! Kritische Sicherheitslücke in GitLab ermöglicht Accountklau

Der Fehler wird bereits aktiv von Kriminellen ausgenutzt, Administratoren sollten zügig handeln und ihre GitLab-Instanzen aktualisieren oder abschotten.

- Link

—

Splunk, cacti, checkmk: Sicherheitslücken in Monitoring-Software

In drei beliebten Monitoring-Produkten gibt es Sicherheitsprobleme. Admins sollten sich um Updates kümmern.

- Link

—

Juniper Networks bessert zahlreiche Schwachstellen aus

Juniper Networks hat 27 Sicherheitsmitteilungen veröffentlicht. Sie betreffen Junos OS, Junos OS Evolved und diverse Hardware.

- Link

—

Sicherheitspatch: IBM Security Verify für Root-Attacken anfällig

Die Entwickler haben in IBMs Zugriffsmanagementlösung Security Verify mehrere Sicherheitslücken geschlossen.

- Link

—

Zoho ManageEngine: Kritische Sicherheitslücke in ADSelfService Plus

In Zoho ManageEngine ADSelfService Plus klafft eine kritische Sicherheitslücke. Angreifer können dadurch Schadcode einschleusen.

- Link

—

Sicherheitsupdates für Dell- und Lenovo-BIOS

Dell stellt aktualisierte BIOS-Versionen für einige Geräte bereit. AMI schließt mehrere Sicherheitslücken, Lenovo reicht die Korrekturen durch.

- 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-2023-5360	0.967230000	0.995830000	Link
CVE-2023-4966	0.925220000	0.987920000	Link
CVE-2023-46747	0.965530000	0.995240000	Link
CVE-2023-46604	0.971470000	0.997580000	Link
CVE-2023-42793	0.972830000	0.998370000	Link
CVE-2023-38035	0.971630000	0.997650000	Link
CVE-2023-35078	0.953380000	0.992020000	Link
CVE-2023-34634	0.906880000	0.985860000	Link
CVE-2023-33246	0.971220000	0.997480000	Link
CVE-2023-32315	0.963520000	0.994490000	Link
CVE-2023-30625	0.937080000	0.989400000	Link
CVE-2023-30013	0.925700000	0.988000000	Link
CVE-2023-29300	0.933050000	0.988910000	Link
CVE-2023-28771	0.923800000	0.987750000	Link
CVE-2023-27524	0.962250000	0.994080000	Link
CVE-2023-27372	0.970430000	0.997040000	Link
CVE-2023-27350	0.972430000	0.998130000	Link
CVE-2023-26469	0.938510000	0.989550000	Link
CVE-2023-26360	0.942270000	0.990030000	Link
CVE-2023-26035	0.968020000	0.996130000	Link
CVE-2023-25717	0.956130000	0.992640000	Link
CVE-2023-25194	0.910840000	0.986280000	Link
CVE-2023-2479	0.958820000	0.993260000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-24489	0.968380000	0.996250000	Link
CVE-2023-23752	0.961870000	0.993990000	Link
CVE-2023-22518	0.965250000	0.995090000	Link
CVE-2023-22515	0.957080000	0.992880000	Link
CVE-2023-21839	0.962040000	0.994050000	Link
CVE-2023-21823	0.940060000	0.989740000	Link
CVE-2023-21554	0.961220000	0.993780000	Link
CVE-2023-20887	0.963250000	0.994400000	Link
CVE-2023-1671	0.953130000	0.991960000	Link
CVE-2023-0669	0.968210000	0.996180000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 16 Jan 2024

[NEU] [hoch] Atlassian Confluence: Mehrere Schwachstellen ermöglichen Codeausführung

Ein Angreifer kann mehrere Schwachstellen in Atlassian Confluence ausnutzen, um beliebigen Code auszuführen.

- Link

—

Tue, 16 Jan 2024

[NEU] [hoch] VMware Cloud Foundation: Schwachstelle ermöglicht Umgehung von Sicherheitsvorkehrungen

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in VMware Cloud Foundation ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Tue, 16 Jan 2024

[NEU] [hoch] Atlassian Bamboo: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Atlassian Bamboo ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, beliebigen Code auszuführen, vertrauliche Informationen

offenzulegen oder einen Request Smuggling-Angriff durchzuführen.

- Link

—

Tue, 16 Jan 2024

[UPDATE] [kritisch] Ruby on Rails: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Ruby on Rails ausnutzen, um Sicherheitsvorkehrungen zu umgehen, Informationen offenzulegen, beliebigen Programmcode auszuführen oder Dateien zu manipulieren.

- Link

—

Tue, 16 Jan 2024

[UPDATE] [kritisch] FreeType: Schwachstelle ermöglicht Codeausführung

Ein entfernter Angreifer kann eine Schwachstelle in FreeType und Xming ausnutzen, um beliebigen Programmcode auszuführen und um einen Denial of Service Zustand herbeizuführen.

- Link

—

Tue, 16 Jan 2024

[UPDATE] [hoch] zlib: Schwachstelle ermöglicht nicht spezifizierten Angriff

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in zlib ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Tue, 16 Jan 2024

[UPDATE] [hoch] Samba: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Samba ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Tue, 16 Jan 2024

[UPDATE] [hoch] binutils: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in binutils ausnutzen, um einen Denial of Service Angriff durchzuführen, Informationen offenzulegen oder sonstige Auswirkungen zu verursachen.

- Link

—

Tue, 16 Jan 2024

[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

—

Tue, 16 Jan 2024

[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

—

Tue, 16 Jan 2024

[UPDATE] [hoch] Microsoft Developer Tools: Mehrere Schwachstellen

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Microsoft Developer Tools ausnutzen, um seine Privilegien zu erhöhen, einen Denial of Service Zustand hervorzurufen oder Sicherheitsmaßnahmen zu umgehen.
- Link

—

Tue, 16 Jan 2024

[NEU] [hoch] Atlassian Confluence Data Center und Server: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Atlassian Confluence ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Mon, 15 Jan 2024

[NEU] [hoch] Paessler PRTG: Schwachstelle ermöglicht Cross-Site Scripting

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Paessler PRTG ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen oder Sicherheitsvorkehrungen zu umgehen.
- Link

—

Mon, 15 Jan 2024

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in git ausnutzen, um Sicherheitsvorkehrungen zu umgehen und beliebigen Code auszuführen.
- Link

—

Mon, 15 Jan 2024

[UPDATE] [hoch] cURL: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in cURL ausnutzen, um Sicherheitsvorkehrungen zu umgehen und einen Denial of Service Zustand herzustellen.

- Link

—

Mon, 15 Jan 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand auszulösen, seine Privilegien zu erweitern und Daten zu manipulieren.

- Link

—

Mon, 15 Jan 2024

[UPDATE] [hoch] OpenSSH: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Mon, 15 Jan 2024

[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in AMD Prozessoren ausnutzen, um beliebigen Programmcode auszuführen oder Informationen offenzulegen.

- Link

—

Mon, 15 Jan 2024

[UPDATE] [hoch] Squid: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Squid ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.

- Link

—

Mon, 15 Jan 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um vertrauliche Informationen offenzulegen oder einen nicht näher spezifizierten Angriff zu starten.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
1/16/2024	[EulerOS 2.0 SP9 : kernel (EulerOS-SA-2023-3304)]	critical
1/16/2024	[EulerOS Virtualization 2.11.0 : scipy (EulerOS-SA-2023-3080)]	critical
1/16/2024	[EulerOS 2.0 SP11 : curl (EulerOS-SA-2023-3267)]	critical
1/16/2024	[EulerOS 2.0 SP10 : curl (EulerOS-SA-2024-1055)]	critical
1/16/2024	[Slackware Linux 15.0 / current xorg-server Multiple Vulnerabilities (SSA:2024-016-02)]	critical
1/16/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : X.Org X Server vulnerabilities (USN-6587-1)]	critical
1/16/2024	[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : ZooKeeper vulnerabilities (USN-6559-1)]	critical
1/16/2024	[Debian dla-3711 : linux-config-5.10 - security update]	critical
1/16/2024	[Debian dla-3710 : hyperv-daemons - security update]	critical
1/16/2024	[EulerOS 2.0 SP11 : docker-runc (EulerOS-SA-2023-2638)]	high
1/16/2024	[EulerOS 2.0 SP10 : qemu-micro (EulerOS-SA-2023-3193)]	high
1/16/2024	[EulerOS 2.0 SP11 : python3 (EulerOS-SA-2023-2705)]	high
1/16/2024	[EulerOS Virtualization 2.11.0 : vim (EulerOS-SA-2023-2777)]	high
1/16/2024	[EulerOS 2.0 SP10 : httpd (EulerOS-SA-2024-1085)]	high
1/16/2024	[EulerOS 2.0 SP11 : vim (EulerOS-SA-2023-2672)]	high
1/16/2024	[EulerOS Virtualization 2.9.0 : libX11 (EulerOS-SA-2024-1015)]	high
1/16/2024	[EulerOS Virtualization 2.10.0 : samba (EulerOS-SA-2023-3482)]	high
1/16/2024	[EulerOS Virtualization 2.9.0 : kernel (EulerOS-SA-2023-3099)]	high
1/16/2024	[EulerOS Virtualization 2.9.0 : vim (EulerOS-SA-2023-2998)]	high

Datum	Schwachstelle	Bewertung
1/16/2024	[NetScaler ADC and NetScaler Gateway Multiple Vulnerabilities (CTX584986l)]	high
1/16/2024	[Rocky Linux 8 : sqlite (RLSA-2024:0253)]	high
1/16/2024	[Security Updates for Microsoft Office Products (Jan 2024) (macOS)]	high
1/16/2024	[RHEL 9 : Red Hat OpenStack Platform 17.1 (python-django) (RHSA-2024:0212)]	high
1/16/2024	[RHEL 9 : Red Hat OpenStack Platform 17.1 (python-werkzeug) (RHSA-2024:0214)]	high
1/16/2024	[RHEL 7 : kernel (RHSA-2024:0261)]	high
1/16/2024	[RHEL 9 : Red Hat OpenStack Platform 17.1 (python-eventlet) (RHSA-2024:0213)]	high
1/16/2024	[RHEL 9 : Red Hat OpenStack Platform 17.1 (openstack-tripleo-common) (RHSA-2024:0216)]	high
1/16/2024	[RHEL 7 : kernel (RHSA-2024:0262)]	high
1/16/2024	[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : FreeImage vulnerabilities (USN-6586-1)]	high
1/16/2024	[Oracle Linux 8 : sqlite (ELSA-2024-0253)]	high
1/16/2024	[Debian dsa-5598 : chromium - security update]	high
1/16/2024	[Amazon Corretto Java 11.x < 11.0.22.7.1 Multiple Vulnerabilities]	high
1/16/2024	[Siemens (CVE-2023-42797)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Tue, 16 Jan 2024

MailCarrier 2.51 Denial Of Service

MailCarrier version 2.51 remote denial of service exploit.

- Link

—

” “Tue, 16 Jan 2024

LightFTP 1.1 Denial Of Service

LightFTP version 1.1 remote denial of service exploit.

- Link

—

” “Mon, 15 Jan 2024

Korenix JetNet Series Unauthenticated Access

Korenix JetNet Series allows TFTP without authentication and also allows for unauthenticated firmware upgrades.

- Link

—

” “Mon, 15 Jan 2024

WordPress RSVPMaker 9.3.2 SQL Injection

WordPress RSVPMaker plugin versions 9.3.2 and below suffer from a remote SQL injection vulnerability.

- Link

—

” “Mon, 15 Jan 2024

Taokeyun SQL Injection

Taokeyun versions up to 1.0.5 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 15 Jan 2024

HaoKeKeJi YiQiNiu Server-Side Request Forgery

HaoKeKeJi YiQiNiu versions up to 3.1 suffer from a server-side request forgery vulnerability.

- Link

—

” “Mon, 15 Jan 2024

Xitami 2.5 Denial Of Service

Xitami version 2.5 remote denial of service exploit.

- Link

—

” “Sun, 14 Jan 2024

freeSSHd 1.0.9 Denial Of Service

freeSSHd version 1.0.9 remote denial of service exploit.

- Link

—

” “Sat, 13 Jan 2024

ProSSHD 1.2 20090726 Denial Of Service

ProSSHD version 1.2 20090726 remote denial of service exploit.

- Link

—

” “Fri, 12 Jan 2024

macOS AppleVADriver Out-Of-Bounds Write

macOS suffers from an out-of-bounds write vulnerability in AppleVADriver when decoding mpeg2 videos.

- Link

—

” “Fri, 12 Jan 2024

macOS AppleGVA Memory Handling

On Intel macOS, HEVC video decoding is performed in the AppleGVA module. Using fuzzing, researchers identified multiple issues in this decoder. The issues range from out-of-bounds writes, out-of-bounds reads and, in one case, free() on an invalid address. All of the issues were reproduced on macOS Ventura 13.6 running on a 2018 Mac mini (Intel based).

- Link

—

” “Fri, 12 Jan 2024

Linux 4.20 KTLS Read-Only Write

Linux versions 4.20 and above have an issue where ktls writes into spliced readonly pages.

- Link

—

” “Fri, 12 Jan 2024

Linux Broken Unix GC Interaction Use-After-Free

Linux suffers from an io_uring use-after-free vulnerability due to broken unix GC interaction.

- Link

—

” “Fri, 12 Jan 2024

Quick TFTP Server Pro 2.1 Denial Of Service

Quick TFTP Server Pro version 2.1 remote denial of service exploit.

- Link

—

” “Fri, 12 Jan 2024

Copyright Loan Management System 2024 1.0 SQL Injection

Copyright Loan Management System 2024 version 1.0 suffers from a remote SQL Injection vulnerabi-

lity that allows for authentication bypass.

- Link

—

” “Thu, 11 Jan 2024

WordPress POST SMTP Mailer 2.8.7 Authorization Bypass / Cross Site Scripting

WordPress POST SMTP Mailer plugin versions 2.8.7 and below suffer from authorization bypass and cross site scripting vulnerabilities.

- Link

—

” “Thu, 11 Jan 2024

SimpleWebServer 2.2-rc2 Denial Of Service

SimpleWebServer version 2.2-rc2 remote denial of service exploit.

- Link

—

” “Thu, 11 Jan 2024

PHPJabbers Event Ticketing System 1.0 Missing Rate Limiting

PHPJabbers Event Ticketing System version 1.0 suffers from a missing rate limiting vulnerability.

- Link

—

” “Thu, 11 Jan 2024

PHPJabbers Meeting Room Booking System 1.0 CSV Injection

PHPJabbers Meeting Room Booking System version 1.0 suffers from a CSV injection vulnerability.

- Link

—

” “Thu, 11 Jan 2024

PHPJabbers Meeting Room Booking System 1.0 Cross Site Scripting

PHPJabbers Meeting Room Booking System version 1.0 suffers from multiple persistent cross site scripting vulnerabilities.

- Link

—

” “Thu, 11 Jan 2024

PHPJabbers Event Ticketing System 1.0 Cross Site Scripting / HTML Injection

PHPJabbers Event Ticketing System version 1.0 suffers from cross site scripting and html injection vulnerabilities.

- Link

—

” “Thu, 11 Jan 2024

PHPJabbers Cinema Booking System 1.0 Missing Rate Limiting

PHPJabbers Cinema Booking System version 1.0 suffers from a missing rate limiting vulnerability.
- Link

—

” “Thu, 11 Jan 2024

PHPJabbers Cinema Booking System 1.0 CSV Injection

PHPJabbers Cinema Booking System version 1.0 suffers from a CSV injection vulnerability.
- Link

—

” “Thu, 11 Jan 2024

PHPJabbers Meeting Room Booking System 1.0 Missing Rate Limiting

PHPJabbers Meeting Room Booking System version 1.0 suffers from a missing rate limiting vulnerability.
- Link

—

” “Thu, 11 Jan 2024

PHPJabbers Cleaning Business Software 1.0 CSV Injection

PHPJabbers Cleaning Business Software version 1.0 suffers from a CSV injection vulnerability.
- Link

—

”

4.2 0-Days der letzten 5 Tage

“Mon, 15 Jan 2024

ZDI-24-073: Paessler PRTG Network Monitor Cross-Site Scripting Authentication Bypass Vulnerability
- Link

—

” “Mon, 15 Jan 2024

ZDI-24-072: Synology RT6600ax Qualcomm LDB Service Improper Input Validation Remote Code Execution Vulnerability
- Link

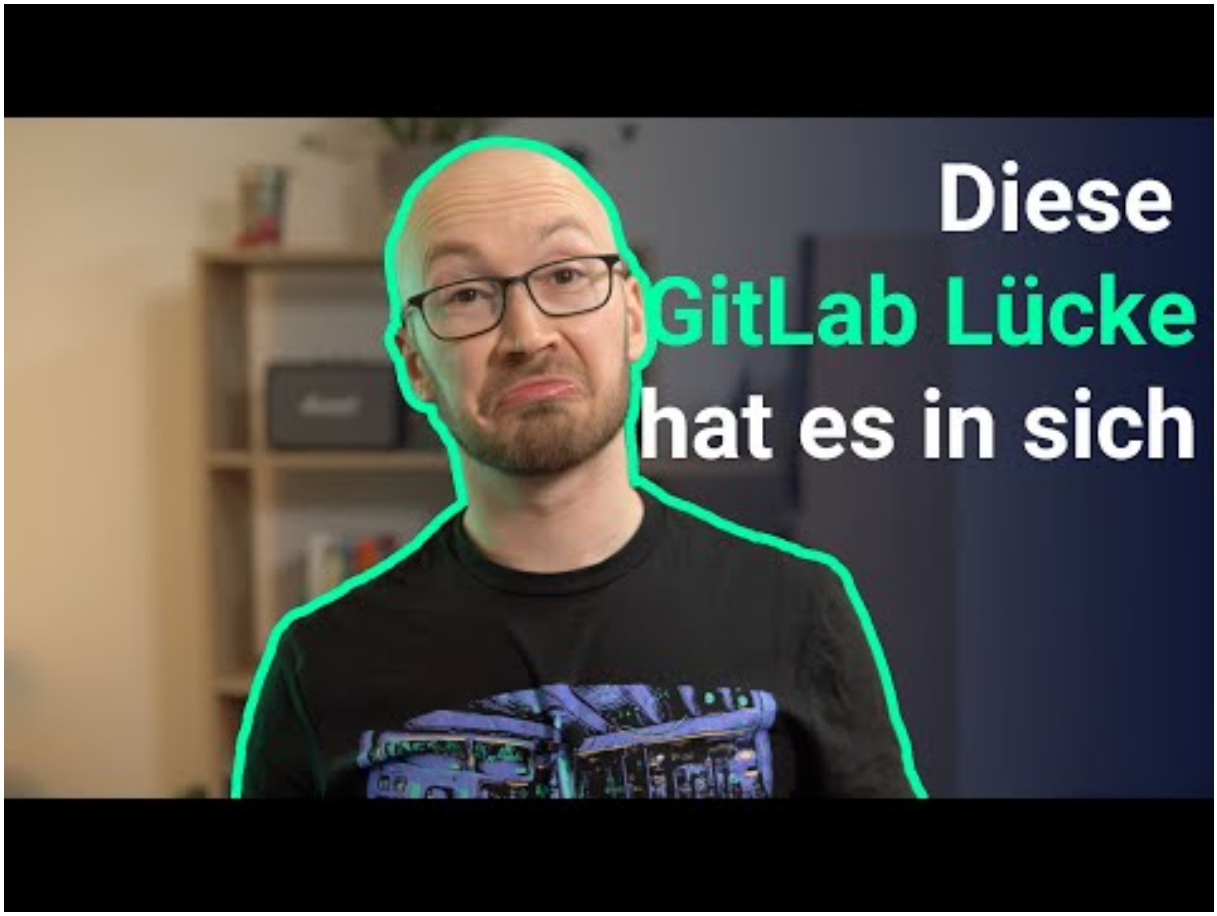
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 WILDE GitLab Lücke (jeden Account übernehmen) & Probleme mit dem AI Hype



Zum Youtube Video

6 Cyberangriffe: (Jan)

Datum	Opfer	Land	Information
2024-01-15	Jingding (□□)	[TWN]	Link
2024-01-13	Calvia	[ESP]	Link
2024-01-13	Sambr'Habitat	[BEL]	Link
2024-01-10	RE&S Holdings	[JPN]	Link
2024-01-10	Lush	[GBR]	Link
2024-01-06	loanDepot	[USA]	Link
2024-01-05	Toronto Zoo	[CAN]	Link
2024-01-05	ODAV AG	[DEU]	Link
2024-01-04	City of Beckley	[USA]	Link
2024-01-04	Tigo Business	[PRY]	Link
2024-01-01	Commune de Saint-Philippe	[FRA]	Link

7 Ransomware-Erpressungen: (Jan)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-17	[JspPharma]	insame	Link
2024-01-16	[Axfast AB]	8base	Link
2024-01-16	[Syndicat Général des Vignerons de la Champagne]	8base	Link
2024-01-16	[Washtech]	8base	Link
2024-01-16	[SIVAM Coatings S.p.A.]	8base	Link
2024-01-16	[Nexus Telecom Switzerland AG]	8base	Link
2024-01-16	[millgate.co.uk]	lockbit3	Link
2024-01-16	[Becker Logistics]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-16	[Bestway Sales]	akira	Link
2024-01-16	[TGS Transportation]	akira	Link
2024-01-16	[Premium Guard]	akira	Link
2024-01-16	[F J O'Hara & Sons]	qilin	Link
2024-01-16	[Donear Industries]	bianlian	Link
2024-01-15	[Beit Handesai]	malekteam	Link
2024-01-15	[shinwajpn.co.jp]	lockbit3	Link
2024-01-15	[maisonsdelavenir.com]	lockbit3	Link
2024-01-15	[vasudhapharma.com]	lockbit3	Link
2024-01-15	[hosted-it.co.uk]	lockbit3	Link
2024-01-15	[Ausa]	hunters	Link
2024-01-15	[Republic Shipping Consolidators, Inc]	bianlian	Link
2024-01-15	[Northeast Spine and Sports Medicine's]	bianlian	Link
2024-01-14	[SPARTAN Light Metal Products]	unsafe	Link
2024-01-14	[Hartl European Transport Company]	unsafe	Link
2024-01-14	[American International College]	unsafe	Link
2024-01-14	[www.kai.id "FF"]	stormous	Link
2024-01-14	[amenitek.com]	lockbit3	Link
2024-01-08	[turascandinavia.com]	lockbit3	Link
2024-01-13	[Lee Spring]	rhysida	Link
2024-01-11	[Charm Sciences]	snatch	Link
2024-01-11	[Malabar Gold & Diamonds]	snatch	Link
2024-01-11	[Banco Promerica]	snatch	Link
2024-01-12	[arrowinternational.com]	lockbit3	Link
2024-01-12	[thecsi.com]	threeam	Link
2024-01-12	[pharrusa.com]	threeam	Link
2024-01-12	[Builcore]	alphv	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-12	[hotelcontinental.no]	qilin	Link
2024-01-12	[olea.com]	lockbit3	Link
2024-01-12	[asburyauto.com]	cactus	Link
2024-01-12	[Washington School For The Deaf]	incransom	Link
2024-01-12	[Former S.p.A.]	8base	Link
2024-01-12	[International Trade Brokers and Forwarders]	8base	Link
2024-01-12	[BALLAY MENUISERIES]	8base	Link
2024-01-12	[Anderson King Energy Consultants, LLC]	8base	Link
2024-01-12	[Sems and Specials Incorporated]	8base	Link
2024-01-12	[acutis.com]	cactus	Link
2024-01-12	[dtsolutions.net]	cactus	Link
2024-01-12	[intercityinvestments.com]	cactus	Link
2024-01-12	[hi-cone.com]	cactus	Link
2024-01-12	[Alliedwoundcare]	everest	Link
2024-01-12	[Primeimaging]	everest	Link
2024-01-11	[Blackburn College]	akira	Link
2024-01-11	[Vincentz Network]	akira	Link
2024-01-11	[Limburg]	medusa	Link
2024-01-11	[Water For People]	medusa	Link
2024-01-11	[pactchangeslives.com]	lockbit3	Link
2024-01-11	[Triella]	alphv	Link
2024-01-11	[Ursel Phillips Fellows Hopkinson]	alphv	Link
2024-01-11	[SHIBLEY RIGHTON]	alphv	Link
2024-01-11	[automotionshade.com]	alphv	Link
2024-01-11	[R Robertson Insurance Brokers]	alphv	Link
2024-01-10	[molnar&partner]	qilin	Link
2024-01-10	[hartalega.com.my]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-10	[agnesb.eu]	lockbit3	Link
2024-01-10	[twt.co.za]	lockbit3	Link
2024-01-10	[tiautoinvestments.co.za]	lockbit3	Link
2024-01-10	[Group Bogart]	alphv	Link
2024-01-09	[Delco Automation]	blacksuit	Link
2024-01-09	[Viridi]	akira	Link
2024-01-09	[Ito Pallpack Gruppen]	akira	Link
2024-01-09	[Corinth Coca-Cola Bottling Works]	qilin	Link
2024-01-09	[Precision Tune Auto Care]	8base	Link
2024-01-08	[Erbilbil Bilgisayar]	alphv	Link
2024-01-08	[HALLEONARD]	qilin	Link
2024-01-08	[Van Buren Public Schools]	akira	Link
2024-01-08	[Heller Industries]	akira	Link
2024-01-08	[CellNetix Pathology & Laboratories, LLC]	incransom	Link
2024-01-08	[mciwv.com]	lockbit3	Link
2024-01-08	[morganpilate.com]	lockbit3	Link
2024-01-07	[capitalhealth.org]	lockbit3	Link
2024-01-07	[Flash-Motors Last Warning]	raznatovic	Link
2024-01-07	[Agro Baggio LTDA]	knight	Link
2024-01-06	[Maas911.com]	cloak	Link
2024-01-06	[GRUPO SCA]	knight	Link
2024-01-06	[Televerde]	play	Link
2024-01-06	[The Lutheran World Federation]	rhysida	Link
2024-01-05	[Proax Technologies LTD]	bianlian	Link
2024-01-05	[Somerset Logistics]	bianlian	Link
2024-01-05	[ips-securex.com]	lockbit3	Link
2024-01-04	[Project M.O.R.E.]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-04	[Thermosash Commercial Ltd]	hunters	Link
2024-01-04	[Gunning & LaFazia, Inc.]	hunters	Link
2024-01-04	[Diablo Valley Oncology and Hematology Medical Group - Press Release]	monti	Link
2024-01-03	[Kershaw County School District]	blacksuit	Link
2024-01-03	[Bradford Health]	hunters	Link
2024-01-02	[groupe-idea.com]	lockbit3	Link
2024-01-02	[SAED International]	alphv	Link
2024-01-02	[graebener-group.com]	blackbasta	Link
2024-01-02	[leonardsexpress.com]	blackbasta	Link
2024-01-02	[nals.com]	blackbasta	Link
2024-01-02	[MPM Medical Supply]	ciphbit	Link
2024-01-01	[DELPHINUS.COM]	clop	Link
2024-01-01	[Aspiration Training]	rhysida	Link
2024-01-01	[Southeast Vermont Transit (MOOver)]	bianlian	Link

8 Quellen

8.1 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

9 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.