Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240119

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

Angreifer attackieren Ivanti EPMM und MobileIron Core

Angreifer nutzen derzeit eine kritische Sicherheitslücke in Ivanti EPMM und MobileIron Core aus.

- Link

—

Nextcloud: Lücken in Apps gefährden Nutzerkonten und Datensicherheit

In mehreren Erweiterungen, etwa zur Lastverteilung, zur Anmeldung per OAuth und ZIP-Download, klaffen Löcher. Updates sind bereits verfügbar.

- Link

—

Trend Micro: Sicherheitslücken in Security-Agents ermöglichen Rechteausweitung

Trend Micro warnt vor Sicherheitslücken in den Security-Agents, durch die Angreifer ihre Rechte ausweiten können. Software-Updates stehen bereit.

- Link

—

MOVEit Transfer: Updates gegen DOS-Lücke

Updates für MOVEit Transfer dichten Sicherheitslecks ab, durch die Angreifer Rechenfehler provozieren oder den Dienst lahmlegen können.

- Link

—

Critical Patch Update: Oracle veröffentlicht 389 Sicherheitsupdates

Oracle hat in seinem Quartalsupdate unter anderem Banking Enterprise, MySQL und Solaris gegen mögliche Angriffe abgesichert.

- Link

—

Jetzt patchen! Vorsicht vor DoS-Angriffen auf Citrix NetScaler ADC und Gateway

Citrix hat Produkte seiner NetScaler-Serie auf den aktuellen Stand gebracht und gegen laufende Attacken gerüstet.

- Link

—

Google Chrome: Sicherheitslücke wird in freier Wildbahn ausgenutzt

Google aktualisiert den Webbrowser Chrome. Das Update schließt hochriskante Sicherheitslücken. Eine davon wird bereits missbraucht.

- Link

—

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

—

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-2023-6553	0.909010000	0.986160000	Link
CVE-2023-5360	0.967230000	0.995850000	Link
CVE-2023-4966	0.925220000	0.987970000	Link
CVE-2023-46805	0.924140000	0.987840000	Link
CVE-2023-46747	0.965530000	0.995250000	Link
CVE-2023-46604	0.971470000	0.997590000	Link
CVE-2023-42793	0.972830000	0.998380000	Link
CVE-2023-38035	0.971630000	0.997660000	Link
CVE-2023-35078	0.953380000	0.992050000	Link
CVE-2023-34634	0.906880000	0.985910000	Link
CVE-2023-33246	0.971220000	0.997490000	Link
CVE-2023-32315	0.963520000	0.994510000	Link
CVE-2023-30625	0.937080000	0.989440000	Link
CVE-2023-30013	0.925700000	0.988050000	Link
CVE-2023-29300	0.936380000	0.989330000	Link
CVE-2023-28771	0.923800000	0.987800000	Link
CVE-2023-27524	0.962250000	0.994100000	Link
CVE-2023-27372	0.969410000	0.996680000	Link
CVE-2023-27350	0.972430000	0.998150000	Link
CVE-2023-26469	0.938510000	0.989590000	Link
CVE-2023-26360	0.940990000	0.989900000	Link
CVE-2023-26035	0.968020000	0.996160000	Link
CVE-2023-25717	0.956130000	0.992670000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-25194	0.910840000	0.986330000	Link
CVE-2023-2479	0.958820000	0.993290000	Link
CVE-2023-24489	0.968380000	0.996270000	Link
CVE-2023-23752	0.963140000	0.994390000	Link
CVE-2023-22518	0.965250000	0.995100000	Link
CVE-2023-22515	0.957080000	0.992910000	Link
CVE-2023-21839	0.962040000	0.994070000	Link
CVE-2023-21823	0.940060000	0.989780000	Link
CVE-2023-21554	0.961220000	0.993810000	Link
CVE-2023-20887	0.963250000	0.994420000	Link
CVE-2023-1671	0.953130000	0.991990000	Link
CVE-2023-0669	0.968210000	0.996210000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Thu, 18 Jan 2024

[NEU] [hoch] Nextcloud: Mehrere Schwachstellen

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Nextcloud Server und verschiedenen Apps ausnutzen, um Benutzerrechte zu erlangen, um den Benutzer zu täuschen und um Sicherheitsmechanismen zu umgehen.

- Link

—

Thu, 18 Jan 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um einen Denial of Service Angriff durchzuführen oder um möglicherweise beliebigen Code auszuführen.

- Link

—

Thu, 18 Jan 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um seine Privilegien zu erhöhen und um einen Denial of Service Zustand herbeizuführen.

- Link

—

Thu, 18 Jan 2024

[UPDATE] [hoch] PostgreSQL: Mehrere Schwachstellen

Ein lokaler oder entfernter authenitisierter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um seine Privilegien zu erhöhen, vertrauliche Daten einzusehen, Daten zu manipulieren, einen Denial of Serivce auszulösen oder Sicherheitsmechanismen zu umgehen.

- Link

—

Thu, 18 Jan 2024

[UPDATE] [hoch] OpenSSL: Mehrere Schwachstellen ermöglichen Denial of Service

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

- Link

—

Thu, 18 Jan 2024

[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

—

Thu, 18 Jan 2024

[UPDATE] [hoch] OpenSSL: Schwachstelle ermöglicht Offenlegung von Informationen

Ein Angreifer kann eine Schwachstelle in OpenSSL ausnutzen, um Informationen offenzulegen.

- Link

—

Thu, 18 Jan 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Thu, 18 Jan 2024

[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um

die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- Link

—

Thu, 18 Jan 2024

[UPDATE] [hoch] Eclipse Jetty: Mehrere Schwachstellen ermöglichen Denial of Service

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Eclipse Jetty ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Thu, 18 Jan 2024

[UPDATE] [hoch] GStreamer: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in GStreamer ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder beliebigen Code auszuführen.

- Link

—

Thu, 18 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

—

Thu, 18 Jan 2024

[UPDATE] [hoch] IBM Business Automation Workflow: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in IBM Business Automation Workflow ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen, einen Denial of Service Zustand herbeizuführen oder Dateien zu manipulieren.

- Link

—

Thu, 18 Jan 2024

[UPDATE] [hoch] Google Chrome & Microsoft Edge: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Thu, 18 Jan 2024

[UPDATE] [hoch] X.Org X11: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in X.Org X11 ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Wed, 17 Jan 2024

[UPDATE] [hoch] IBM QRadar SIEM: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in IBM QRadar SIEM ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen, Informationen falsch darzustellen, einen Denial of Service Zustand herbeizuführen, Sicherheitsvorkehrungen zu umgehen, einen Cross-Site-Scripting-Angriff durchzuführen oder unbekannte Auswirkungen zu verursachen.
- Link

—

Wed, 17 Jan 2024

[UPDATE] [kritisch] Apache Struts: Schwachstelle ermöglicht Codeausführung

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

—

Wed, 17 Jan 2024

[NEU] [hoch] Citrix Systems Produkte: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Citrix Systems ADC und Citrix Systems Citrix Gateway ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service zu verursachen.
- Link

—

Wed, 17 Jan 2024

[NEU] [hoch] EDK2 NetworkPkg IP stack implementation: Mehrere Schwachstellen

Ein Angreifer aus dem angrenzenden Netzwerk oder ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der EDK2 NetworkPkg IP stack implementation ausnutzen, um beliebigen Programmcode auszuführen, vertrauliche Informationen offenzulegen und einen Denial of Service Zustand auszulösen.
- Link

—

Wed, 17 Jan 2024

[NEU] [hoch] Oracle Enterprise Manager: Mehrere Schwachstellen

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

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
1/19/2024	[openSUSE 15 Security Update : libuev (openSUSE-SU-2024:0023-1)]	critical
1/19/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : libqt5-qtbase (SUSE-SU-2024:0138-1)]	critical
1/18/2024	[Oracle HTTP Server Multiple Vulnerabilities (January 2024 CPU)]	critical
1/18/2024	[Oracle Linux 8 : .NET / 6.0 (ELSA-2024-0158)]	critical
1/19/2024	[SUSE SLES15 Security Update : kernel (SUSE-SU-2024:0153-1)]	high
1/19/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : perl-Spreadsheet-ParseExcel (SUSE-SU-2024:0158-1)]	high
1/19/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : libcryptopp (SUSE-SU-2024:0157-1)]	high
1/19/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2024:0160-1)]	high
1/19/2024	[SUSE SLES15 Security Update : suse-module-tools (SUSE-SU-2024:0155-1)]	high
1/19/2024	[SUSE SLED15 / SLES15 Security Update : kernel (SUSE-SU-2024:0156-1)]	high
1/19/2024	[SUSE SLES15 Security Update : kernel (SUSE-SU-2024:0154-1)]	high
1/19/2024	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2024:0141-1)]	high
1/19/2024	[Fedora 38 : chromium (2024-049f068a8c)]	high

Datum	Schwachstelle	Bewertung
1/19/2024	[Fedora 39 : golang-github-facebook-time (2024-07c811c7a5)]	high
1/19/2024	[Fedora 38 : golang-github-facebook-time (2024-f99ecead66)]	high
1/19/2024	[Fedora 39 : chromium (2024-44b1f656a3)]	high
1/19/2024	[Fedora 39 : xorg-x11-server-Xwayland (2024-da3d410b53)]	high
1/18/2024	[RHEL 8 / 9 : OpenShift Container Platform 4.14.9 (RHSA-2024:0207)]	high
1/18/2024	[RHEL 8 : OpenShift Container Platform 4.12.47 (RHSA-2024:0200)]	high
1/18/2024	[Oracle WebLogic Server (January 2024 CPU)]	high
1/18/2024	[ManageEngine ADSelfService Plus < build 6402 Authenticated RCE]	high
1/18/2024	[Oracle Linux 8 / 9 : python3.11-cryptography (ELSA-2024-12078)]	high
1/18/2024	[Oracle Application Testing Suite DoS (January 2024 CPU)]	high
1/18/2024	[Progress MOVEit Transfer < 2022.0.10 / 2022.1 < 2022.1.11 / 2023.0 < 2023.0.8 / 2023.1 < 2023.1.3 Multiple Vulnerabilities (January 2024)]	high
1/18/2024	[Oracle Primavera P6 Enterprise Project Portfolio Management (January 2024 CPU)]	high
1/18/2024	[Oracle Primavera Unifier (January 2024 CPU)]	high
1/18/2024	[UltraVNC < 1.3.8.1 Privilege Escalation]	high
1/18/2024	[Amazon Linux 2 : java-17-amazon-corretto (ALAS-2024-2415)]	high
1/18/2024	[Amazon Linux 2 : java-11-amazon-corretto (ALAS-2024-2414)]	high
1/18/2024	[RHEL 8 / 9 : java-11-openjdk (RHSA-2024:0266)]	high
1/18/2024	[RHEL 8 : python-urllib3 (RHSA-2024:0300)]	high

Datum	Schwachstelle	Bewertung
1/18/2024	[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS : Xerces-C++ vulnerabilities (USN-6590-1)]	high
1/18/2024	[Amazon Linux 2023 : java-1.8.0-amazon-corretto, java-1.8.0-amazon-corretto-devel (ALAS2023-2024-482)]	high
1/18/2024	[Amazon Linux 2023 : java-21-amazon-corretto, java-21-amazon-corretto-devel, java-21-amazon-corretto-headless (ALAS2023-2024-485)]	high
1/18/2024	[Amazon Linux 2023 : java-11-amazon-corretto, java-11-amazon-corretto-devel, java-11-amazon-corretto-headless (ALAS2023-2024-484)]	high
1/18/2024	[Amazon Linux 2023 : java-17-amazon-corretto, java-17-amazon-corretto-devel, java-17-amazon-corretto-headless (ALAS2023-2024-483)]	high
1/18/2024	[Oracle Linux 8 : python-cryptography (ELSA-2024-12079)]	high
1/18/2024	[Oracle Linux 7 : gstreamer-plugins-bad-free (ELSA-2024-0279)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Thu, 18 Jan 2024

WordPress Backup Migration 1.3.7 Remote Command Execution

This Metasploit module exploits an unauthenticated remote command execution vulnerability in WordPress Backup Migration plugin versions 1.3.7 and below. The vulnerability is exploitable through the Content-Dir header which is sent to the /wp-content/plugins/backup-backup/includes/backup-heart.php endpoint. The exploit makes use of a neat technique called PHP Filter Chaining which allows an attacker to prepend bytes to a string by continuously chaining character encoding conversions. This allows an attacker to prepend a PHP payload to a string which gets evaluated by a require statement, which results in command execution.

- Link

—

” “Thu, 18 Jan 2024

Ansible Agent Payload Deployer

This exploit module creates an ansible module for deployment to nodes in the network. It creates a new yaml playbook which copies our payload, chmods it, then runs it on all targets which have been selected (default all).

- Link

—

” “Thu, 18 Jan 2024

SpyCamLizard 1.230 Denial Of Service

SpyCamLizard version 1.230 remote denial of service exploit.

- Link

—

” “Thu, 18 Jan 2024

Legends Of IdleOn Random Number Generation Manipulation

Legends of IdleOn suffers from use of an insecure random number generator that can be replaced by a malicious user.

- Link

—

” “Wed, 17 Jan 2024

Easy File Sharing FTP 3.6 Denial Of Service

Easy File Sharing FTP version 3.6 remote denial of service exploit.

- Link

—

” “Wed, 17 Jan 2024

PixieFail Proof Of Concepts

This archive contains proof of concepts to trigger the 7 vulnerabilities in Tianocore’s EDK II open source implementation of the UEFI specification. Issues include an integer underflow, buffer overflows, infinite loops, and an out of bounds read.

- Link

—

” “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 vulnerability 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
—
”

4.2 0-Days der letzten 5 Tage

“Fri, 19 Jan 2024
ZDI-24-080: Trend Micro Mobile Security for Enterprises vpplist_assign_list Cross-Site Scripting Vulnerability
- Link
—
” “Fri, 19 Jan 2024
ZDI-24-079: Trend Micro Mobile Security for Enterprises ServerUpdate_UpdateSuccessful Cross-Site Scripting Vulnerability
- Link
—
” “Fri, 19 Jan 2024
ZDI-24-078: Trend Micro Mobile Security for Enterprises DevicesManagementEditNotePopupTip Cross-Site Scripting Vulnerability
- Link
—
” “Fri, 19 Jan 2024

ZDI-24-077: Trend Micro Apex Central Unrestricted File Upload Vulnerability

- Link

—

” “Fri, 19 Jan 2024

ZDI-24-076: Trend Micro Deep Security Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Fri, 19 Jan 2024

ZDI-24-075: Trend Micro Deep Security Improper Access Control Local Privilege Escalation Vulnerability

- Link

—

” “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

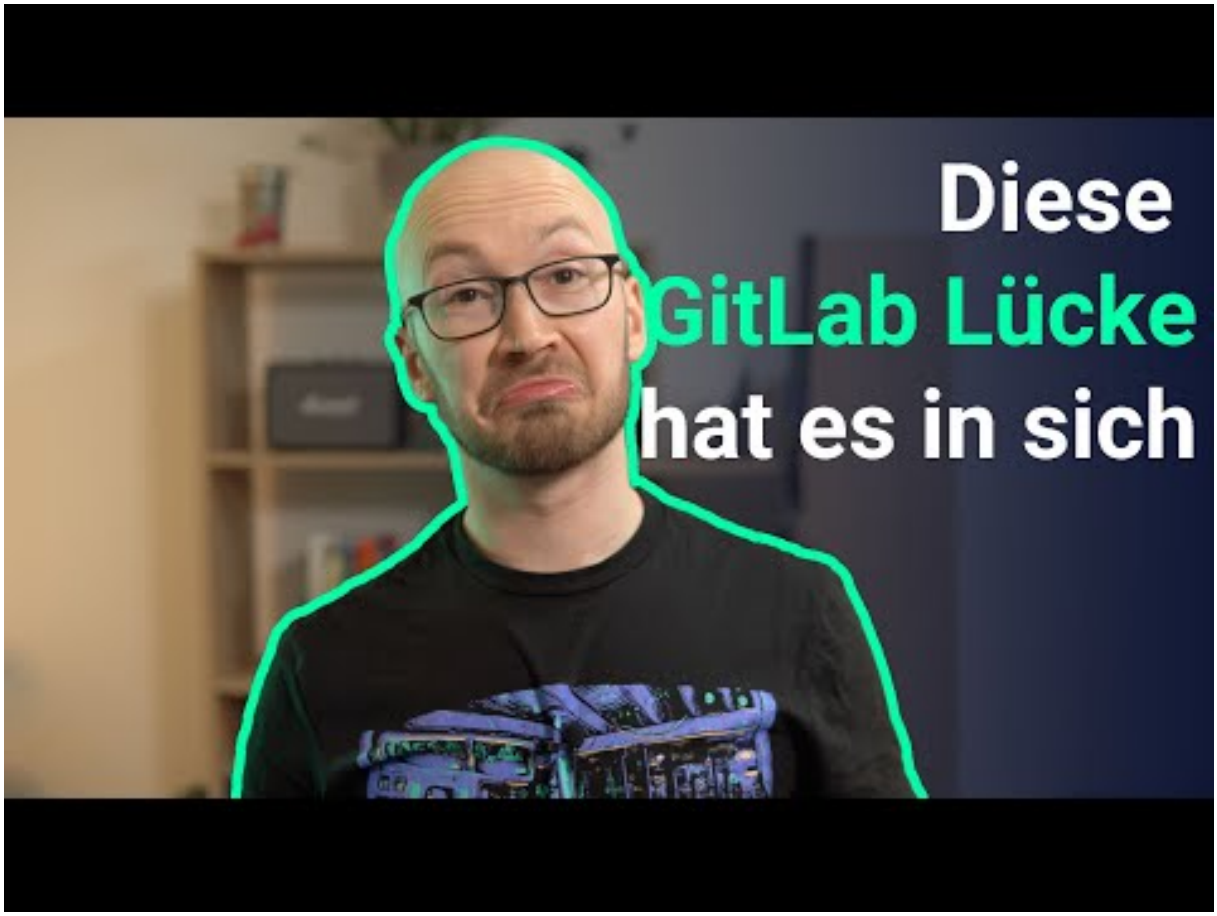
—

”

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
2024-01-17	Donau 3 FM	[DEU]	Link
2024-01-17	Service de secours de Jämtland	[SWE]	Link
2024-01-16	Université d'État du Kansas (K-State)	[USA]	Link
2024-01-15	Foxsemicon Integrated Technology Inc (□□□□)	[TWN]	Link
2024-01-15	Canterbury City Council, Thanet District Council, Dover District Council.	[GBR]	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
2024-01-06	Banque nationale d'Angola	[AGO]	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
2024-01-18	[Samuel Sekuritas Indonesia & Samuel Aset Manajemen]	trigona	Link
2024-01-18	[Premier Facility Management]	trigona	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-18	[Fertility North]	trigona	Link
2024-01-18	[Vision Plast]	trigona	Link
2024-01-18	[uffs.edu.br]	stormous	Link
2024-01-18	[Groveport Madison Schools]	blacksuit	Link
2024-01-18	[GROWTH by NCRC]	bianlian	Link
2024-01-18	[LT Business Dynamics]	bianlian	Link
2024-01-18	[digipwr.com]	lockbit3	Link
2024-01-18	[jaffeandasher.com]	lockbit3	Link
2024-01-18	[Gallup McKinley County Schools]	hunters	Link
2024-01-15	[aercap.com]	slug	Link
2024-01-17	[DENHAM the Jeanmaker]	akira	Link
2024-01-17	[Stone, Avant & Daniels]	medusa	Link
2024-01-17	[JspPharma]	insane	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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.