Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240308

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

VMware schließt Schlupflöcher für Ausbruch aus virtueller Maschine

Angreifer können Systeme mit VMware ESXi, Fusion und Workstation attackieren. Sicherheitsupdates stehen zum Download.

- Link

—

Sicherheitslücken: Angreifer können Systeme mit IBM-Software attackieren

Es gibt wichtige Sicherheitsupdates für IBM Business Automation Workflow und IBM WebSphere-Komponenten. Es kann Schadcode auf Systeme gelangen.

- Link

—

Google Chrome: Update dichtet drei hochriskante Sicherheitslecks ab

Google hat mit einer aktualisierten Chrome-Browser-Version drei Sicherheitslücken geschlossen. Sie gelten als hohes Risiko.

- Link

—

Jetzt updaten: Kritische Admin-Sicherheitslücken bedrohen TeamCity

Angreifer können die volle Kontrolle über die Software-Build-Plattform TeamCity erlangen. Sicherheitspatches stehen zum Download.

- Link

—

Patchday: Kritische Schadcode-Lücken bedrohen Android 12, 13 und 14

Google und andere Hersteller haben für bestimmte Android-Geräte wichtige Sicherheitsupdates veröffentlicht.

- Link

—

Angreifer können Systeme mit Dell-Software kompromittieren

Es sind wichtige Sicherheitspatches für Dell Data Protection Advisor, iDRAC8 und Secure Connect Gateway erschienen.

- Link

—

Solarwinds: Schadcode-Lücke in Security Event Manager

Sicherheitslücken in Solarwinds Secure Event Manager können Angreifer zum Einschleusen von Schadcode missbrauchen. Updates stopfen die Lecks.

- Link

—

Aruba: Codeschmuggel durch Sicherheitslücken im Clearpass Manager möglich

Im Aruba Clearpass Manager von HPE klaffen teils kritische Sicherheitslücken. Updates zum Schließen stehen bereit.

- Link

—

Angriffe auf Windows-Lücke – Update seit einem halben Jahr verfügbar

Die CISA warnt vor Angriffen auf eine Lücke in Microsofts Streaming Service. Updates gibt es seit mehr als einem halben Jahr.

- Link

—

Sicherheitsupdate: Nividia-Grafikkarten-Treiber als Einfallstor für Angreifer

Angreifer können Linux- und Windows-PCs mit Nvidia-GPUs ins Visier nehmen. Es kann Schadcode auf Systeme gelangen.

- 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-2023-6895	0.901600000	0.987140000	Link
CVE-2023-6553	0.916210000	0.988300000	Link
CVE-2023-5360	0.967230000	0.996330000	Link
CVE-2023-4966	0.963970000	0.995270000	Link
CVE-2023-47246	0.943540000	0.991420000	Link
CVE-2023-46805	0.962740000	0.994880000	Link
CVE-2023-46747	0.972020000	0.998020000	Link
CVE-2023-46604	0.972730000	0.998390000	Link
CVE-2023-43177	0.927670000	0.989600000	Link
CVE-2023-42793	0.973450000	0.998840000	Link
CVE-2023-41265	0.923180000	0.989020000	Link
CVE-2023-39143	0.925430000	0.989310000	Link
CVE-2023-38646	0.904440000	0.987300000	Link
CVE-2023-38205	0.934710000	0.990280000	Link
CVE-2023-38203	0.959860000	0.994240000	Link
CVE-2023-38035	0.972370000	0.998260000	Link
CVE-2023-36845	0.966580000	0.996100000	Link
CVE-2023-3519	0.911860000	0.987920000	Link
CVE-2023-35082	0.934310000	0.990240000	Link
CVE-2023-35078	0.948280000	0.992140000	Link
CVE-2023-34960	0.925010000	0.989270000	Link
CVE-2023-34634	0.919000000	0.988590000	Link
CVE-2023-34362	0.959040000	0.994020000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34039	0.917140000	0.988390000	Link
CVE-2023-3368	0.904650000	0.987320000	Link
CVE-2023-33246	0.973410000	0.998790000	Link
CVE-2023-32315	0.973960000	0.999120000	Link
CVE-2023-30625	0.946250000	0.991770000	Link
CVE-2023-30013	0.937480000	0.990610000	Link
CVE-2023-29300	0.963530000	0.995130000	Link
CVE-2023-29298	0.921360000	0.988810000	Link
CVE-2023-28771	0.923800000	0.989130000	Link
CVE-2023-28121	0.925190000	0.989300000	Link
CVE-2023-27524	0.972470000	0.998280000	Link
CVE-2023-27372	0.971320000	0.997740000	Link
CVE-2023-27350	0.972270000	0.998200000	Link
CVE-2023-26469	0.938970000	0.990790000	Link
CVE-2023-26360	0.960730000	0.994470000	Link
CVE-2023-26035	0.970030000	0.997160000	Link
CVE-2023-25717	0.962180000	0.994740000	Link
CVE-2023-2479	0.963310000	0.995070000	Link
CVE-2023-24489	0.973430000	0.998820000	Link
CVE-2023-23752	0.948570000	0.992190000	Link
CVE-2023-23397	0.917330000	0.988410000	Link
CVE-2023-22527	0.965680000	0.995870000	Link
CVE-2023-22518	0.970110000	0.997190000	Link
CVE-2023-22515	0.973330000	0.998760000	Link
CVE-2023-21839	0.960490000	0.994430000	Link
CVE-2023-21554	0.961220000	0.994550000	Link
CVE-2023-20887	0.965640000	0.995850000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-20198	0.919220000	0.988600000	Link
CVE-2023-1671	0.964380000	0.995390000	Link
CVE-2023-0669	0.968020000	0.996580000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Thu, 07 Mar 2024

[NEU] [hoch] pgAdmin: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Thu, 07 Mar 2024

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

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

- Link

—

Thu, 07 Mar 2024

[NEU] [hoch] JFrog Artifactory: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in JFrog Artifactory ausnutzen, um Informationen offenzulegen.

- Link

—

Thu, 07 Mar 2024

[UPDATE] [hoch] Checkmk: Schwachstelle ermöglicht Privilegienerweiterung

Ein Angreifer kann eine Schwachstelle in Checkmk ausnutzen, um seine Privilegien zu erweitern.

- Link

—

Thu, 07 Mar 2024

[UPDATE] [hoch] Veritas NetBackup: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Veritas NetBackup ausnutzen, um

beliebigen Programmcode auszuführen.
- Link

—

Thu, 07 Mar 2024

[UPDATE] [hoch] vim: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und Dateien zu manipulieren.
- Link

—

Thu, 07 Mar 2024

[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

Thu, 07 Mar 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, 07 Mar 2024

[UPDATE] [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

—

Thu, 07 Mar 2024

[UPDATE] [hoch] Red Hat JBoss A-MQ: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat JBoss A-MQ und Red Hat Enterprise Linux ausnutzen, um Informationen offenzulegen oder beliebigen Programmcode auszuführen.
- Link

—

Thu, 07 Mar 2024

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in PostgreSQL ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Thu, 07 Mar 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder um Sicherheitsmaßnahmen zu umgehen.

- Link

—

Thu, 07 Mar 2024

[UPDATE] [hoch] IBM WebSphere Service Registry and Repository: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in IBM WebSphere Service Registry and Repository ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen oder vertrauliche Informationen offenzulegen.

- Link

—

Thu, 07 Mar 2024

[NEU] [hoch] IBM Power Hardware Management Console: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in IBM Power Hardware Management Console ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen, Dateien zu manipulieren oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Thu, 07 Mar 2024

[NEU] [hoch] Cisco Secure Client: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Cisco Secure Client ausnutzen, um Benutzerrechte zu erlangen oder seine Privilegien zu erweitern.

- Link

—

Thu, 07 Mar 2024

[NEU] [hoch] Jenkins: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Jenkins ausnutzen, um Sicherheitsvorkehrungen zu umgehen, Informationen offenzulegen, Dateien zu manipulieren oder einen Cross-Site-Scripting-Angriff durchzuführen.

- Link

—

Wed, 06 Mar 2024

[NEU] [hoch] VMware Produkte: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in VMware ESXi, VMware Workstation, VMware Fusion und VMware Cloud Foundation ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsvorkehrungen zu umgehen oder Informationen offenzulegen.

- Link

—

Wed, 06 Mar 2024

[NEU] [hoch] Moxa NPort: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Moxa NPort ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Wed, 06 Mar 2024

[NEU] [hoch] Apple iOS: Mehrere Schwachstellen

Ein anonymer Angreifer kann mehrere Schwachstellen in Apple iOS ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.

- Link

—

Wed, 06 Mar 2024

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

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

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
3/7/2024	[SUSE SLES12 Security Update : postgresql-jdbc (SUSE-SU-2024:0771-1)]	critical
3/7/2024	[VMware ESXi 7.0 / 8.0 Multiple Vulnerabilities (VMSA-2024-0006)]	critical

Datum	Schwachstelle	Bewertung
3/7/2024	[Ubuntu 20.04 LTS / 22.04 LTS : Puma vulnerabilities (USN-6682-1)]	critical
3/7/2024	[Oracle Linux 9 : kernel (ELSA-2024-0461)]	critical
3/7/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2014-0069)]	high
3/7/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2013-6381)]	high
3/7/2024	[CBL Mariner 2.0 Security Update: qt5-qtbase / qt5-qtsvg (CVE-2021-38593)]	high
3/7/2024	[AlmaLinux 9 : haproxy (ALSA-2024:1142)]	high
3/7/2024	[OracleVM 3.4 : kernel-uek (OVMSA-2024-0003)]	high
3/7/2024	[AlmaLinux 9 : golang (ALSA-2024:1131)]	high
3/7/2024	[AlmaLinux 9 : tomcat (ALSA-2024:1134)]	high
3/7/2024	[CentOS 8 : thunderbird (CESA-2024:0964)]	high
3/7/2024	[CentOS 8 : firefox (CESA-2024:0955)]	high
3/7/2024	[Oracle Linux 8 : kernel (ELSA-2024-0897)]	high
3/7/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : giflib (SUSE-SU-2024:0786-1)]	high
3/7/2024	[SUSE SLES12 Security Update : gstreamer-plugins-bad (SUSE-SU-2024:0779-1)]	high
3/7/2024	[SUSE SLES12 Security Update : xmlgraphics-batik (SUSE-SU-2024:0777-1)]	high
3/7/2024	[SUSE SLES12 Security Update : vim (SUSE-SU-2024:0783-1)]	high
3/7/2024	[SUSE SLES12 Security Update : apache2-mod_auth_openidc (SUSE-SU-2024:0758-1)]	high
3/7/2024	[SUSE SLES15 Security Update : gstreamer-plugins-bad (SUSE-SU-2024:0780-1)]	high
3/7/2024	[IBM HTTP Server 8.5.0.0 < 8.5.5.26 / 9.0.0.0 < 9.0.5.18 DoS (7129933)]	high
3/7/2024	[Cisco Secure Client Carriage Return Line Feed Injection (cisco-sa-secure-client-crlf-W43V4G7)]	high

Datum	Schwachstelle	Bewertung
3/7/2024	[Golang < 1.33.0 DOS]	high
3/7/2024	[ArubaOS < 8.10.0.10 / 8.11.2.1 / 10.4.1.0 / 10.5.1.0 Multiple Vulnerabilities (ARUBA-PSA-2024-002)]	high
3/7/2024	[macOS 14.x < 14.4 Multiple Vulnerabilities (HT214084)]	high
3/7/2024	[macOS 12.x < 12.7.4 Multiple Vulnerabilities (HT214083)]	high
3/7/2024	[Foxit PDF Reader for Mac < 2024.1 Multiple Vulnerabilities]	high
3/7/2024	[Foxit PDF Editor for Mac < 2024.1 Multiple Vulnerabilities]	high
3/7/2024	[Microsoft Edge (Chromium) < 122.0.2365.80 Multiple Vulnerabilities]	high
3/7/2024	[AlmaLinux 9 : mysql (ALSA-2024:1141)]	high
3/7/2024	[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : HtmlCleaner vulnerability (USN-6683-1)]	high
3/7/2024	[Slackware Linux 15.0 / current ghostscript Vulnerability (SSA:2024-067-01)]	high
3/7/2024	[RHEL 8 : openvswitch3.1 (RHSA-2024:1235)]	high
3/7/2024	[RHEL 9 : openvswitch3.1 (RHSA-2024:1227)]	high
3/7/2024	[RHEL 8 : openvswitch2.17 (RHSA-2024:1234)]	high
3/7/2024	[Oracle Linux 9 : tomcat (ELSA-2024-1134)]	high
3/7/2024	[macOS 13.x < 13.6.5 Multiple Vulnerabilities (HT214085)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Wed, 06 Mar 2024

Artica Proxy 4.50 Loopback Service Disclosure

Services that are running and bound to the loopback interface on the Artica Proxy version 4.50 are accessible through the proxy service. In particular, the tailon service is running as the root user, is bound to the loopback interface, and is listening on TCP port 7050. Using the tailon service, the contents of any file on the Artica Proxy can be viewed.

- Link

—

” “Wed, 06 Mar 2024

Artica Proxy 4.40 / 4.50 Authentication Bypass / Privilege Escalation

The Rich Filemanager feature of Artica Proxy versions 4.40 and 4.50 provides a web-based interface for file management capabilities. When the feature is enabled, it does not require authentication by default, and runs as the root user. This provides an unauthenticated attacker complete access to the file system.

- Link

—

” “Wed, 06 Mar 2024

Artica Proxy 4.50 Unauthenticated PHP Deserialization

The Artica Proxy administrative web application will deserialize arbitrary PHP objects supplied by unauthenticated users and subsequently enable code execution as the www-data user. Version 4.50 is affected.

- Link

—

” “Wed, 06 Mar 2024

Artica Proxy 4.40 / 4.50 Local File Inclusion / Traversal

Artica Proxy versions 4.40 and 4.50 suffer from a local file inclusion protection bypass vulnerability that allows for path traversal.

- Link

—

” “Wed, 06 Mar 2024

JetBrains TeamCity Authentication Bypass / Remote Code Execution

JetBrains TeamCity versions prior to 2023.11.4 remote authentication bypass exploit that can be leveraged for user addition and remote code execution.

- Link

—

” “Wed, 06 Mar 2024

F5 BIG-IP Authorization Bypass / User Creation

F5 BIG-IP remote user addition exploit that leverages the authorization bypass vulnerability as called out in CVE-2023-46747.

- Link

—

” “Wed, 06 Mar 2024

Customer Support System 1.0 SQL Injection

Customer Support System version 1.0 suffers from a remote SQL injection vulnerability in /custo-

mer_support/ajax.php. Original discovery of SQL injection in this version is attributed to Ahmed Abbas in November of 2020.

- Link

—

” “Tue, 05 Mar 2024

RAD SecFlow-2 Path Traversal

RAD SecFlow-2 devices with Hardware 0202, Firmware 4.1.01.63, and U-Boot 2010.12 suffer from a directory traversal vulnerability.

- Link

—

” “Tue, 05 Mar 2024

Solar-Log 200 PM+ 3.6.0 Cross Site Scripting

Solar-Log 200 PM+ version 3.6.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 05 Mar 2024

WordPress Neon Text 1.1 Cross Site Scripting

WordPress Neon Text plugin versions 1.1 and below suffer from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 05 Mar 2024

KK Star Ratings Race Condition

KK Star Ratings versions prior to 5.4.6 suffer from rate tampering via a race condition vulnerability.

- Link

—

” “Mon, 04 Mar 2024

BoidCMS 2.0.1 Cross Site Scripting

BoidCMS version 2.0.1 suffers from multiple cross site scripting vulnerabilities. Original discovery of cross site scripting in this version is attributed to Rahad Chowdhury in December of 2023, though this advisory provides additional vectors of attack.

- Link

—

” “Mon, 04 Mar 2024

TP-Link JetStream Smart Switch TL-SG2210P 5.0 Build 20211201 Privilege Escalation

TP-Link JetStream Smart Switch TL-SG2210P version 5.0 build 20211201 suffers from a privilege escalation vulnerability.

- Link

—

” “Mon, 04 Mar 2024

Wallos Shell Upload

Wallos versions prior to 1.11.2 suffer from a remote shell upload vulnerability.

- Link

—

” “Mon, 04 Mar 2024

Petrol Pump Management System 1.0 Shell Upload

Petrol Pump Management System version 1.0 suffers from a remote shell upload vulnerability. This is a variant vector of attack in comparison to the original discovery attributed to SoSPiro in February of 2024.

- Link

—

” “Mon, 04 Mar 2024

Petrol Pump Management Software 1.0 SQL Injection

Petrol Pump Management Software version 1.0 suffers from a remote SQL injectionvulnerability.

- Link

—

” “Mon, 04 Mar 2024

Petrol Pump Management Software 1.0 Cross Site Scripting

Petrol Pump Management Software version 1.0 suffers from multiple cross site scripting vulnerabilities.

- Link

—

” “Mon, 04 Mar 2024

Easywall 0.3.1 Remote Command Execution

Easywall version 0.3.1 suffers from an authenticated remote command execution vulnerability.

- Link

—

” “Mon, 04 Mar 2024

GL.iNet AR300M 3.216 Remote Code Execution

GL.iNet AR300M versions 3.216 and below suffer from an OpenVPN client related remote code execution vulnerability.

- Link

—

” “Mon, 04 Mar 2024

GL.iNet AR300M 4.3.7 Remote Code Execution

GL.iNet AR300M versions 4.3.7 and below suffer from an OpenVPN client related remote code executi-

on vulnerability.
- Link
—
” “Mon, 04 Mar 2024
GL.iNet AR300M 4.3.7 Arbitrary File Write
GL.iNet AR300M versions 4.3.7 and below suffer from an arbitrary file writing vulnerability.
- Link
—
” “Mon, 04 Mar 2024
SumatraPDF 3.5.2 DLL Hijacking
SumatraPDF version 3.5.2 suffers from a DLL hijacking vulnerability using CRYPTBASE.DLL. DLL hijacking in this version was already discovered by Ravishanka Silva in February of 2024 but the findings did not include this DLL.
- Link
—
” “Mon, 04 Mar 2024
Employee Management System 1.0-2024 SQL Injection
Employee Management System version 1.0-2024 suffers from a remote SQL injection vulnerability. Original discovery of this finding is attributed to Ozlem Balci in January of 2024.
- Link
—
” “Mon, 04 Mar 2024
TPC-110W Missing Authentication
TPC-110W suffers from a missing authentication vulnerability.
- Link
—
” “Mon, 04 Mar 2024
Boss Mini 1.4.0 Local File Inclusion
Boss Mini version 1.4.0 suffers from a local file inclusion vulnerability.
- Link
—
”

4.2 0-Days der letzten 5 Tage

“Tue, 05 Mar 2024
ZDI-24-249: (0Day) Ashlar-Vellum Cobalt IGS File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 05 Mar 2024

ZDI-24-248: (0Day) Ashlar-Vellum Cobalt IGS File Parsing Type Confusion Remote Code Execution Vulnerability

- Link

—

” “Tue, 05 Mar 2024

ZDI-24-247: (0Day) Ashlar-Vellum Cobalt STP File Parsing Uninitialized Pointer Remote Code Execution Vulnerability

- Link

—

” “Tue, 05 Mar 2024

ZDI-24-246: (0Day) Ashlar-Vellum Cobalt STP File Parsing Type Confusion Remote Code Execution Vulnerability

- Link

—

” “Tue, 05 Mar 2024

ZDI-24-245: (0Day) Ashlar-Vellum Cobalt STP File Parsing Uninitialized Pointer Remote Code Execution Vulnerability

- Link

—

” “Tue, 05 Mar 2024

ZDI-24-244: (0Day) Ashlar-Vellum Cobalt STP File Parsing Type Confusion Remote Code Execution Vulnerability

- Link

—

” “Tue, 05 Mar 2024

ZDI-24-243: (0Day) Ashlar-Vellum Cobalt STP File Parsing Type Confusion Remote Code Execution Vulnerability

- Link

—

” “Tue, 05 Mar 2024

ZDI-24-242: (0Day) Ashlar-Vellum Cobalt STP File Parsing Type Confusion Remote Code Execution Vulnerability

- Link

—

” “Tue, 05 Mar 2024

ZDI-24-241: (0Day) Ashlar-Vellum Cobalt STP File Parsing Type Confusion Remote Code Execution Vulnerability

- Link

—

” “Tue, 05 Mar 2024

ZDI-24-240: (0Day) Ashlar-Vellum Cobalt STP File Parsing Type Confusion Remote Code Execution Vulnerability

- Link

—

” “Tue, 05 Mar 2024

ZDI-24-239: (0Day) Ashlar-Vellum Cobalt STP File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 05 Mar 2024

ZDI-24-238: (0Day) Ashlar-Vellum Cobalt STP File Parsing Type Confusion Remote Code Execution Vulnerability

- Link

—

” “Tue, 05 Mar 2024

ZDI-24-237: (0Day) Ashlar-Vellum Cobalt STP File Parsing Type Confusion Remote Code Execution Vulnerability

- Link

—

” “Tue, 05 Mar 2024

ZDI-24-236: (0Day) Ashlar-Vellum Cobalt STP File Parsing Type Confusion Remote Code Execution Vulnerability

- Link

—

” “Tue, 05 Mar 2024

ZDI-24-235: (0Day) Ashlar-Vellum Cobalt STP File Parsing Type Confusion Remote Code Execution Vulnerability

- Link

—

” “Tue, 05 Mar 2024

ZDI-24-234: (0Day) Ashlar-Vellum Cobalt STP File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 04 Mar 2024

ZDI-24-233: Delta Electronics CNCSoft-B DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 04 Mar 2024

ZDI-24-232: Kofax Power PDF JPG File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Mon, 04 Mar 2024

ZDI-24-231: Kofax Power PDF PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Mon, 04 Mar 2024

ZDI-24-230: Kofax Power PDF TIF File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Come on, ALPHV... Das Gesundheitssystem?

Zum Youtube Video

6 Cyberangriffe: (Mär)

Datum	Opfer	Land	Information
2024-03-06	Brasserie Duvel Moortgat	[BEL]	Link
2024-03-04	FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)	[CAN]	Link
2024-03-04	South St. Paul Public Schools	[USA]	Link
2024-03-01	Hansab	[EST]	Link

7 Ransomware-Erpressungen: (Mär)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-07	[rmhfranchise.com]	lockbit3	Link
2024-03-07	[New York Home Healthcare]	bianlian	Link
2024-03-07	[Palmer Construction Co., Inc]	bianlian	Link
2024-03-07	[en-act-architecture]	qilin	Link
2024-03-07	[Merchant ID]	ransomhub	Link
2024-03-07	[SP Mundi]	ransomhub	Link
2024-03-07	[www.duvel.com]	stormous	Link
2024-03-06	[www.loghmanpharma.com]	stormous	Link
2024-03-06	[MainVest]	play	Link
2024-03-06	[C?????????? A???????e T???????????]	play	Link
2024-03-05	[Haivision MCS]	medusa	Link
2024-03-06	[Tocci Building Corporation]	medusa	Link
2024-03-06	[JVCKENWOOD]	medusa	Link
2024-03-06	[American Renal Associates]	medusa	Link
2024-03-06	[US #1364 Federal Credit Union]	medusa	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-06	[viadirectamarketing]	stormous	Link
2024-03-06	[Liquid Environmental Solutions]	incransom	Link
2024-03-06	[Infosoft]	akira	Link
2024-03-06	[brightwires.com.sa]	qilin	Link
2024-03-06	[Medical Billing Specialists]	akira	Link
2024-03-06	[Telecentro]	akira	Link
2024-03-06	[Steiner (Austrian furniture makers)]	akira	Link
2024-03-06	[Biomedical Research Institute]	meow	Link
2024-03-06	[K???o???]	play	Link
2024-03-06	[Kudulis Reisinger Price]	8base	Link
2024-03-06	[Global Zone]	8base	Link
2024-03-06	[Mediplast AB]	8base	Link
2024-03-05	[airbogo]	stormous	Link
2024-03-05	[sunwave.com.cn]	lockbit3	Link
2024-03-05	[SJCME.EDU]	clop	Link
2024-03-05	[central.k12.or.us]	lockbit3	Link
2024-03-05	[iemsc.com]	qilin	Link
2024-03-05	[hawita-gruppe]	qilin	Link
2024-03-05	[Future Generations Foundation]	meow	Link
2024-03-04	[Seven Seas Group]	snatch	Link
2024-03-04	[Paul Davis Restoration]	medusa	Link
2024-03-04	[Veeco]	medusa	Link
2024-03-04	[dismogas]	stormous	Link
2024-03-04	[everplast]	stormous	Link
2024-03-04	[DiVal Safety Equipment, Inc.]	hunters	Link
2024-03-04	[America Chung Nam orACN]	akira	Link
2024-03-03	[jovani.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-03	[valoremreply.com]	lockbit3	Link
2024-03-04	[Martin’s, Inc.]	bianlian	Link
2024-03-03	[Prompt Financial Solutions]	medusa	Link
2024-03-03	[Sophiahemmet University]	medusa	Link
2024-03-03	[Centennial Law Group LLP]	medusa	Link
2024-03-03	[Eastern Rio Blanco Metropolitan]	medusa	Link
2024-03-03	[Chris Argiropoulos Professional]	medusa	Link
2024-03-03	[THAISUMMIT.US]	clop	Link
2024-03-03	[THESAFIRCHOICE.COM]	clop	Link
2024-03-03	[ipmaltamira]	alphv	Link
2024-03-03	[earnesthealth.com]	lockbit3	Link
2024-03-03	[Ward Transport & Logistics]	dragonforce	Link
2024-03-03	[Ponoka.ca]	cloak	Link
2024-03-03	[stockdevelopment.com]	lockbit3	Link
2024-03-03	[Ewig Usa]	alphv	Link
2024-03-02	[aerospace.com]	lockbit3	Link
2024-03-02	[starkpower.de]	lockbit3	Link
2024-03-02	[roehr-stolberg.de]	lockbit3	Link
2024-03-02	[schuett-grundei.de]	lockbit3	Link
2024-03-02	[unitednotions.com]	lockbit3	Link
2024-03-02	[smuldes.com]	lockbit3	Link
2024-03-02	[esser-ps.de]	lockbit3	Link
2024-03-01	[SBM & Co [You have 48 hours. Check your e-mail]]	alphv	Link
2024-03-01	[Skyland Grain]	play	Link
2024-03-01	[American Nuts]	play	Link
2024-03-01	[A&A Wireless]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-01	[Powill Manufacturing & Engineering]	play	Link
2024-03-01	[Trans+Plus Systems]	play	Link
2024-03-01	[Hedlunds]	play	Link
2024-03-01	[Red River Title]	play	Link
2024-03-01	[Compact Mould]	play	Link
2024-03-01	[Winona Pattern & Mold]	play	Link
2024-03-01	[Marketon]	play	Link
2024-03-01	[Stack Infrastructure]	play	Link
2024-03-01	[Coastal Car]	play	Link
2024-03-01	[New Bedford Welding Supply]	play	Link
2024-03-01	[Influence Communication]	play	Link
2024-03-01	[Kool-air]	play	Link
2024-03-01	[FBi Construction]	play	Link
2024-03-01	[SBM & Co]	alphv	Link
2024-03-01	[Shooting House]	ransomhub	Link
2024-03-01	[Crystal Window & Door Systems]	dragonforce	Link
2024-03-01	[Gilmore Construction]	blacksuit	Link
2024-03-01	[Petrus Resources Ltd]	alphv	Link
2024-03-01	[CoreData]	akira	Link
2024-03-01	[Gansevoort Hotel Group]	akira	Link
2024-03-01	[DJI Company]	mogilevich	Link
2024-03-01	[Kick]	mogilevich	Link
2024-03-01	[Shein]	mogilevich	Link
2024-03-01	[Kumagai Gumi Group]	alphv	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.