Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240306

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

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

—

IT-Sicherheitsprodukte von Sophos verschlucken sich am Schaltjahr

Aufgrund eines Fehlers können Sophos Endpoint, Home und Server vor dem Besuch legitimer Websites warnen. Erste Lösungen sind bereits verfügbar.

- Link

—

3D-Drucker von Anycubic gehackt, um vor weiteren Hacks zu warnen

Derzeit bekommen einige Besitzer von 3D-Druckern des Herstellers Anycubic eine Warnmeldung auf Geräte geschickt. Diese stammt aber nicht vom Hersteller.

- Link

—

Cisco: Sicherheitslücken in NX-OS, FX-OS und weiteren Geräten geschlossen

Cisco warnt vor Sicherheitslücken in mehreren Systemen und Geräten. Aktualisierungen zum Abdichten stehen bereit.

- 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	0.987110000	Link
CVE-2023-6553	0.916210000	0.988260000	Link
CVE-2023-5360	0.967230000	0.996340000	Link
CVE-2023-4966	0.963970000	0.995270000	Link
CVE-2023-47246	0.943540000	0.991410000	Link
CVE-2023-46805	0.962740000	0.994870000	Link
CVE-2023-46747	0.972020000	0.998020000	Link
CVE-2023-46604	0.972730000	0.998380000	Link
CVE-2023-43177	0.927670000	0.989560000	Link
CVE-2023-42793	0.973450000	0.998830000	Link
CVE-2023-41265	0.923180000	0.988980000	Link
CVE-2023-39143	0.925430000	0.989270000	Link
CVE-2023-38646	0.904440000	0.987280000	Link
CVE-2023-38205	0.934710000	0.990250000	Link
CVE-2023-38203	0.949400000	0.992280000	Link
CVE-2023-38035	0.972370000	0.998260000	Link
CVE-2023-36845	0.966580000	0.996100000	Link
CVE-2023-3519	0.908750000	0.987630000	Link
CVE-2023-35082	0.934310000	0.990220000	Link
CVE-2023-35078	0.948280000	0.992120000	Link
CVE-2023-34960	0.925010000	0.989240000	Link
CVE-2023-34634	0.919000000	0.988550000	Link
CVE-2023-34362	0.959040000	0.994020000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34039	0.917140000	0.988350000	Link
CVE-2023-3368	0.928930000	0.989620000	Link
CVE-2023-33246	0.973410000	0.998780000	Link
CVE-2023-32315	0.973960000	0.999110000	Link
CVE-2023-30625	0.951530000	0.992610000	Link
CVE-2023-30013	0.937480000	0.990600000	Link
CVE-2023-29300	0.963530000	0.995130000	Link
CVE-2023-29298	0.921360000	0.988770000	Link
CVE-2023-28771	0.923800000	0.989100000	Link
CVE-2023-28121	0.925190000	0.989270000	Link
CVE-2023-27524	0.972470000	0.998290000	Link
CVE-2023-27372	0.971580000	0.997830000	Link
CVE-2023-27350	0.972270000	0.998200000	Link
CVE-2023-26469	0.938970000	0.990780000	Link
CVE-2023-26360	0.960730000	0.994460000	Link
CVE-2023-26035	0.970030000	0.997160000	Link
CVE-2023-25717	0.962180000	0.994730000	Link
CVE-2023-2479	0.963310000	0.995060000	Link
CVE-2023-24489	0.973430000	0.998820000	Link
CVE-2023-23752	0.948570000	0.992170000	Link
CVE-2023-23397	0.917330000	0.988380000	Link
CVE-2023-22527	0.965680000	0.995870000	Link
CVE-2023-22518	0.970110000	0.997200000	Link
CVE-2023-22515	0.973330000	0.998750000	Link
CVE-2023-21839	0.960490000	0.994410000	Link
CVE-2023-21554	0.961220000	0.994530000	Link
CVE-2023-20887	0.965640000	0.995850000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-20198	0.919220000	0.988560000	Link
CVE-2023-1671	0.964380000	0.995390000	Link
CVE-2023-0669	0.968020000	0.996580000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 05 Mar 2024

[UPDATE] [hoch] GNU Emacs: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Tue, 05 Mar 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

—

Tue, 05 Mar 2024

[UPDATE] [hoch] IBM MQ: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in IBM MQ ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Tue, 05 Mar 2024

[NEU] [hoch] Android Patchday März

Ein Angreifer kann mehrere Schwachstellen in Google Android und Pixel ausnutzen, um seine Privilegien zu erhöhen, beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Tue, 05 Mar 2024

[NEU] [hoch] Samsung Android: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Samsung Android ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen oder seine Rechte zu erweitern.

- Link

—

Tue, 05 Mar 2024

[NEU] [hoch] Linux: Mehrere Schwachstellen

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

- Link

—

Tue, 05 Mar 2024

[NEU] [hoch] Hashicorp Vault: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Hashicorp Vault ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Tue, 05 Mar 2024

[NEU] [hoch] Squid: Schwachstelle ermöglicht Denial of Service

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

- Link

—

Tue, 05 Mar 2024

[NEU] [hoch] IBM WebSphere Application Server: Mehrere Schwachstellen

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

- Link

—

Tue, 05 Mar 2024

[UPDATE] [hoch] Ruby: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Ruby ausnutzen, um Daten zu manipulieren, vertrauliche Daten einzusehen oder einen Denial of Service Angriff durchzuführen.

- Link

—

Tue, 05 Mar 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit den Rechten des Dienstes

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux und CentOS ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen oder einen Denial of Service zu verursachen.

- Link

—

Tue, 05 Mar 2024

[UPDATE] [hoch] Squid: Schwachstelle ermöglicht Denial of Service

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

- Link

—

Tue, 05 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

—

Tue, 05 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

—

Tue, 05 Mar 2024

[UPDATE] [hoch] Linux “Shim”: Schwachstelle ermöglicht Übernahme der Kontrolle

Ein anonymer Angreifer aus dem angrenzenden Netzwerk kann eine Schwachstelle in der “Shim” Komponente von Linux-Systemen ausnutzen, um die Kontrolle über ein betroffenes System zu übernehmen.

- Link

—

Tue, 05 Mar 2024

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

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

- Link

—

Tue, 05 Mar 2024

[UPDATE] [hoch] Node.js: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder seine Privilegien zu erweitern.

- Link

—

Tue, 05 Mar 2024

[UPDATE] [hoch] Mozilla Firefox, Mozilla Firefox ESR und Mozilla 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 offenzulegen, Sicherheitsmaßnahmen zu umgehen oder einen nicht spezifizierten Angriff durchzuführen.

- Link

—

Tue, 05 Mar 2024

[UPDATE] [hoch] Red Hat Ansible Automation Platform: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat Ansible Automation Platform ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren, Phishing-Angriffe durchzuführen oder Cross-Site Scripting (XSS)-Angriffe auszuführen. Einige dieser Schwachstellen erfordern eine Benutzerinteraktion, um sie erfolgreich auszunutzen.

- Link

—

Tue, 05 Mar 2024

[NEU] [hoch] JetBrains TeamCity: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in JetBrains TeamCity ausnutzen, um bestimmte Aktionen mit administrativen Rechten auszuführen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
3/5/2024	[RHEL 9 : frr (RHSA-2024:1093)]	critical
3/5/2024	[JetBrains TeamCity Authentication Bypass (CVE-2024-27198)]	critical
3/5/2024	[Unitronics VisiLogic < 9.9.00 Default Password]	critical
3/5/2024	[Google Chrome < 122.0.6261.111 Multiple Vulnerabilities]	critical
3/5/2024	[Apple iOS < 16.7.6 Vulnerability (HT214082)]	critical
3/5/2024	[RHEL 8 : emacs (RHSA-2024:1103)]	critical
3/5/2024	[RHEL 9 : frr (RHSA-2024:1152)]	critical
3/5/2024	[RHEL 8 : frr (RHSA-2024:1113)]	critical
3/5/2024	[RHEL 9 : gnutls (RHSA-2024:1082)]	high
3/5/2024	[RHEL 9 : haproxy (RHSA-2024:1089)]	high
3/5/2024	[RHEL 9 : libfastjson (RHSA-2024:1086)]	high
3/5/2024	[RHEL 9 : tomcat (RHSA-2024:1092)]	high
3/5/2024	[RHEL 9 : sqlite (RHSA-2024:1081)]	high
3/5/2024	[RHEL 9 : libX11 (RHSA-2024:1088)]	high
3/5/2024	[Atlassian Bamboo 8.1 < 9.2.7 / 9.3 < 9.3.4 RCE]	high
3/5/2024	[Debian dla-3749 : php-seclib - security update]	high
3/5/2024	[Debian dla-3750 : php-phpseclib - security update]	high
3/5/2024	[Atlassian Confluence 4.1.x < 7.19.17 / 8.0.x < 8.5.4 / 8.6.x < 8.6.2 / 8.7.x < 8.7.2 / 8.8.0 (CONFSERVER-94108)]	high
3/5/2024	[Apple iOS < 17.4 Multiple Vulnerabilities (HT214081)]	high
3/5/2024	[Debian dla-3751 : libapache2-mod-auth-openidc - security update]	high
3/5/2024	[RHEL 9 : haproxy (RHSA-2024:1142)]	high
3/5/2024	[RHEL 9 : tomcat (RHSA-2024:1134)]	high

Datum	Schwachstelle	Bewertung
3/5/2024	[RHEL 8 : gmp (RHSA-2024:1102)]	high
3/5/2024	[RHEL 9 : squid (RHSA-2024:1153)]	high
3/5/2024	[RHEL 9 : mysql (RHSA-2024:1141)]	high
3/5/2024	[RHEL 8 : device-mapper-multipath (RHSA-2024:1110)]	high
3/5/2024	[RHEL 9 : golang (RHSA-2024:1131)]	high
3/5/2024	[RHEL 8 : systemd (RHSA-2024:1105)]	high
3/5/2024	[RHEL 8 : sqlite (RHSA-2024:1107)]	high
3/5/2024	[RHEL 8 : cups (RHSA-2024:1101)]	high
3/5/2024	[RHEL 8 : gnutls (RHSA-2024:1108)]	high
3/5/2024	[RHEL 9 : libfastjson (RHSA-2024:1154)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“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 vulnerabili-

ties.

- 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 execution 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

—

” “Mon, 04 Mar 2024

Multilaser RE160 Cookie Manipulation Access Bypass

Multilaser RE160 versions 5.07.51_pt_MTL01 and 5.07.52_pt_MTL01 suffer from an access control bypass vulnerability through cookie manipulation.

- Link

—

” “Mon, 04 Mar 2024

Multilaser RE160V / RE160 URL Manipulation Access Bypass

Multilaser RE160V web management interface versions 12.03.01.08_pt and 12.03.01.09_pt along with RE160 versions 5.07.51_pt_MTL01 and 5.07.52_pt_MTL01 suffer from an access control bypass vulnerability through URL manipulation.

- Link

—

” “Mon, 04 Mar 2024

Multilaser RE160V Header Manipulation Access Bypass

Multilaser RE160V web management interface versions 12.03.01.09_pt and 12.03.01.10_pt suffer from an access control bypass vulnerability through header manipulation.

- Link

—

” “Mon, 04 Mar 2024

A-PDF All To MP3 Converter 2.0.0 Overflow

A-PDF All to MP3 Converter version 2.0.0 overflow exploit with DEP Bypass with HeapCreate + HeapAlloc + some_memory_copy_function ROP chain.

- Link

—

” “Mon, 04 Mar 2024

Real Estate Management System 1.0 Shell Upload

Real Estate Management System version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Mon, 04 Mar 2024

XAMPP 5.6.40 SQL Injection

XAMPP version 5.6.40 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 04 Mar 2024

Qognify VMS Client Viewer 7.1 DLL Hijacking

Qognify VMS Client Viewer version 7.1 suffers from a local privilege escalation vulnerability via DLL hijacking.

- 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
2024-03-04	FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)	[CAN]	Link
2024-03-01	Hansab	[EST]	Link

7 Ransomware-Erpressungen: (Mär)

Datum	Opfer	Ransomware-Grupppe	Webseite
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-04	[America Chung Nam orACN]	akira	Link
2024-03-03	[jovani.com]	lockbit3	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-01	[American Nuts]	play	Link
2024-03-01	[A&A Wireless]	play	Link
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.