Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240311

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 patchen! Deutschland führt Liste mit verwundbaren TeamCity-Systemen an
Angreifer kompromittieren derzeit gehäuft das Software-Distributionssystem TeamCity. Das kann ein Ausgangspunkt für eine Supply-Chain-Attacke sein.
- Link

—

Cisco: Angreifer können sich zum Root-Nutzer unter Linux machen
Die Softwareentwickler des Netzwerkausrüsters Cisco haben mehrere Sicherheitslücken geschlossen.
- Link

—

macOS 14.4 und mehr: Apple patcht schwere Sicherheitslücken
Auf iOS folgen Apples andere Betriebssysteme: Die Updates schließen gravierende Sicherheitslücken, die offenbar für Angriffe ausgenutzt wurden.
- Link

—

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

—

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	0.987150000	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	0.991430000	Link
CVE-2023-46805	0.962740000	0.994880000	Link
CVE-2023-46747	0.972020000	0.998030000	Link
CVE-2023-46604	0.972730000	0.998390000	Link
CVE-2023-43177	0.927670000	0.989580000	Link
CVE-2023-42793	0.973450000	0.998850000	Link
CVE-2023-41265	0.923180000	0.989000000	Link
CVE-2023-39143	0.925430000	0.989290000	Link
CVE-2023-38646	0.916640000	0.988350000	Link
CVE-2023-38205	0.934710000	0.990280000	Link
CVE-2023-38203	0.959860000	0.994250000	Link
CVE-2023-38035	0.972370000	0.998260000	Link
CVE-2023-36845	0.966580000	0.996110000	Link
CVE-2023-3519	0.911860000	0.987930000	Link
CVE-2023-35082	0.935540000	0.990360000	Link
CVE-2023-35078	0.948280000	0.992140000	Link
CVE-2023-34960	0.929930000	0.989740000	Link
CVE-2023-34634	0.919000000	0.988600000	Link
CVE-2023-34362	0.959040000	0.994040000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34039	0.917140000	0.988400000	Link
CVE-2023-3368	0.904650000	0.987330000	Link
CVE-2023-33246	0.973410000	0.998800000	Link
CVE-2023-32315	0.973840000	0.999040000	Link
CVE-2023-30625	0.946250000	0.991780000	Link
CVE-2023-30013	0.937480000	0.990610000	Link
CVE-2023-29300	0.963690000	0.995180000	Link
CVE-2023-29298	0.921360000	0.988810000	Link
CVE-2023-28771	0.923800000	0.989110000	Link
CVE-2023-28121	0.925190000	0.989280000	Link
CVE-2023-27524	0.972470000	0.998280000	Link
CVE-2023-27372	0.971320000	0.997750000	Link
CVE-2023-27350	0.971970000	0.998010000	Link
CVE-2023-26469	0.938970000	0.990790000	Link
CVE-2023-26360	0.960730000	0.994500000	Link
CVE-2023-26035	0.970030000	0.997170000	Link
CVE-2023-25717	0.962180000	0.994750000	Link
CVE-2023-2479	0.962540000	0.994820000	Link
CVE-2023-24489	0.973400000	0.998800000	Link
CVE-2023-23752	0.948570000	0.992190000	Link
CVE-2023-23397	0.917330000	0.988420000	Link
CVE-2023-22527	0.965680000	0.995890000	Link
CVE-2023-22518	0.970110000	0.997200000	Link
CVE-2023-22515	0.972700000	0.998380000	Link
CVE-2023-21839	0.960490000	0.994450000	Link
CVE-2023-21554	0.961220000	0.994560000	Link
CVE-2023-20887	0.965070000	0.995630000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-20198	0.919220000	0.988610000	Link
CVE-2023-1671	0.964380000	0.995390000	Link
CVE-2023-0669	0.968640000	0.996780000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 08 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

—

Fri, 08 Mar 2024

[UPDATE] [hoch] Red Hat fontforge: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Fri, 08 Mar 2024

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

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um Informationen offenzulegen und Sicherheitsmaßnahmen zu umgehen.

- Link

—

Fri, 08 Mar 2024

[UPDATE] [hoch] Python: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Fri, 08 Mar 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Denial of Service

Ein Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um einen Denial of Service Angriff durchzuführen oder um Informationen offenzulegen.
- Link

—

Fri, 08 Mar 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

—

Fri, 08 Mar 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Fri, 08 Mar 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

—

Fri, 08 Mar 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Fri, 08 Mar 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Fri, 08 Mar 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

—

Fri, 08 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

—

Fri, 08 Mar 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

—

Fri, 08 Mar 2024

[UPDATE] [hoch] Oracle Supply Chain: Mehrere Schwachstellen

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

- Link

—

Fri, 08 Mar 2024

[NEU] [hoch] MongoDB: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein anonymer Angreifer im angrenzenden Netzbereich kann eine Schwachstelle in MongoDB ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Fri, 08 Mar 2024

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

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

- Link

—

Fri, 08 Mar 2024

[NEU] [hoch] Apple macOS: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um vertrauliche Informationen offenzulegen, Dateien zu manipulieren, einen Denial-of-Service-Zustand

zu verursachen, beliebigen Code auszuführen, seine Privilegien zu erweitern oder Sicherheitsmaßnahmen zu umgehen.

- Link

—

Fri, 08 Mar 2024

[NEU] [hoch] Apple Safari: Mehrere Schwachstellen

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

- Link

—

Thu, 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

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
3/9/2024	[SUSE SLES12 Security Update : containerd (SUSE-SU-2024:0799-1)]	critical
3/8/2024	[Android Buffer Overflow in WhatsApp (CVE-2019-3568)]	critical
3/8/2024	[IBM Engineering Requirements Management DOORS 9.7.2.x < 9.7.2.8 Multiple Vulnerabilities (7124058)]	critical

Datum	Schwachstelle	Bewertung
3/10/2024	[Fedora 39 : qpdf (2024-8762164e47)]	critical
3/10/2024	[Fedora 38 : qpdf (2024-daa7df59d6)]	critical
3/9/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : jetty-minimal (SUSE-SU-2024:0817-1)]	high
3/9/2024	[SUSE SLES15 / openSUSE 15 Security Update : python310 (SUSE-SU-2024:0820-1)]	high
3/9/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : go1.21 (SUSE-SU-2024:0811-1)]	high
3/9/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : go1.22 (SUSE-SU-2024:0812-1)]	high
3/9/2024	[SUSE SLES15 Security Update : gstreamer-plugins-bad (SUSE-SU-2024:0793-1)]	high
3/9/2024	[SUSE SLES12 Security Update : java-1_8_0-openjdk (SUSE-SU-2024:0804-1)]	high
3/9/2024	[SUSE SLES12 Security Update : go1.21 (SUSE-SU-2024:0800-1)]	high
3/9/2024	[FreeBSD : Unbound – Denial-of-Service vulnerability (c2ad8700-de25-11ee-9190-84a93843eb75)]	high
3/8/2024	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : mqtt-client vulnerability (USN-6685-1)]	high
3/8/2024	[Ubuntu 22.04 LTS / 23.10 : Linux kernel vulnerabilities (USN-6680-2)]	high
3/8/2024	[FreeBSD : Gitlab – Vulnerabilities (b2caae55-dc38-11ee-96dc-001b217b3468)]	high
3/8/2024	[FreeBSD : electron{27,28} – vulnerability in libxml2 (e74da31b-276a-4a22-9772-17dd42b97559)]	high
3/8/2024	[NVIDIA Virtual GPU Manager Multiple Vulnerabilities (February 2024)]	high
3/8/2024	[NVIDIA Linux GPU Display Driver (February 2024)]	high
3/8/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : xmlgraphics-batik (SUSE-SU-2024:0808-1)]	high

Datum	Schwachstelle	Bewertung
3/8/2024	[openSUSE 15 Security Update : sudo (SUSE-SU-2024:0794-1)]	high
3/8/2024	[openSUSE 15 Security Update : google-oauth-java-client (SUSE-SU-2024:0806-1)]	high
3/8/2024	[RHEL 8 / 9 : Red Hat Ansible Automation Platform 2.4 Product Security and Bug Fix Update (Important) (RHSA-2024:1057)]	high
3/8/2024	[JetBrains TeamCity Path Traversal (CVE-2024-27199)]	high
3/8/2024	[Cisco Secure Client for Linux with ISE Posture Module Privilege Escalation (cisco-sa-secure-privesc-sYxQO6ds)]	high
3/8/2024	[Oracle Linux 9 : edk2 (ELSA-2024-1075)]	high
3/8/2024	[Fedora 38 : chromium (2024-f781c993fe)]	high
3/8/2024	[Cisco NX-OS Buffer Copy without Checking Size of Input (CVE-2024-20267)]	high
3/8/2024	[Cisco NX-OS Allocation of Resources Without Limits or Throttling (CVE-2024-20321)]	high
3/11/2024	[RHEL 9 : postgresql (RHSA-2024:1241)]	high
3/11/2024	[RHEL 9 : postgresql (RHSA-2024:1240)]	high
3/10/2024	[Fedora 39 : exercism (2024-cafa04a149)]	high
3/10/2024	[Debian dla-3756 : wordpress - security update]	high
3/10/2024	[Debian dsa-5638 : libuv1 - security update]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Fri, 08 Mar 2024

MongoDB 2.0.1 / 2.1.1 / 2.1.4 / 2.1.5 Local Password Disclosure

MongoDB versions 2.0.1, 2.1.1, 2.1.4, and 2.1.5 appear to suffer from multiple localized password disclosure issues.

- Link

—

” “Fri, 08 Mar 2024

Ladder 0.0.21 Server-Side Request Forgery

Ladder versions 0.0.1 through 0.0.21 fail to apply sufficient default restrictions on destination addresses, allowing an attacker to make GET requests to addresses that would typically not be accessible from an external context. An attacker can access private address ranges, locally listening services, and cloud instance metadata APIs.

- Link

—

” “Thu, 07 Mar 2024

FullCourt Enterprise 8.2 Cross Site Scripting

FullCourt Enterprise version 8.2 suffers from multiple cross site scripting vulnerabilities.

- Link

—

” “Thu, 07 Mar 2024

NDtaskmatic 1.0 SQL Injection

NDtaskmatic version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Thu, 07 Mar 2024

GliNet 4.x Authentication Bypass

GliNet with firmware version 4.x suffers from an authentication bypass vulnerability. Other firmware versions may also be affected.

- Link

—

” “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 /customer_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 execution vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Fri, 08 Mar 2024

ZDI-24-256: Dassault Systèmes eDrawings CATPART File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 08 Mar 2024

ZDI-24-255: Dassault Systèmes eDrawings X_T File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 08 Mar 2024

ZDI-24-254: Dassault Systèmes eDrawings DWG File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 08 Mar 2024

ZDI-24-253: Dassault Systèmes eDrawings SLDDRW File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 08 Mar 2024

ZDI-24-252: Dassault Systèmes eDrawings JT File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 08 Mar 2024

ZDI-24-251: Dassault Systèmes eDrawings SAT File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Fri, 08 Mar 2024

ZDI-24-250: Dassault Systèmes eDrawings DXF File Parsing Out-Of-Bounds Write 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
2024-03-09	Leicester City Council	[GBR]	Link
2024-03-07	Administradora de Subsidios Sociales (ADESS)	[DOM]	Link
2024-03-07	Beyers Koffie	[BEL]	Link
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
2024-03-11	[Scadea Solutions]	ransomhub	Link
2024-03-09	[https://www.consorzioinnova.it]	alphalocker	Link
2024-03-09	[DVT]	ransomhub	Link
2024-03-09	[Rekamy]	ransomhub	Link
2024-03-09	[go4kora]	ransomhub	Link
2024-03-09	[H + G EDV Vertriebs]	blacksuit	Link
2024-03-09	[Fincasrevuelta]	everest	Link
2024-03-09	[Lindsay Municipal Hospital]	bianlian	Link
2024-03-09	[Group Health Cooperative - Rev 500kk]	blacksuit	Link
2024-03-09	[ACE Air Cargo]	hunters	Link
2024-03-09	[Watsonclinic.com]	donutleaks	Link
2024-03-06	[Continental Aerospace Technologies]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-08	[redwoodcoastrc.org]	lockbit3	Link
2024-03-08	[PowerRail Distribution]	blacksuit	Link
2024-03-08	[Denninger's]	medusa	Link
2024-03-08	[SIEA]	ransomhub	Link
2024-03-08	[Hozzify]	ransomhub	Link
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.