Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240807

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

Sicherheitsupdate: Kritische Schadcode-Lücke bedroht Analyseplattform Kibana
In aktuellen Versionen haben die Kibana-Entwickler ein gefährliches Sicherheitsproblem gelöst.
- Link

—

Patchday: Attacken auf Android-Geräte beobachtet
Google hat mehrere Schwachstellen in seinem mobilen Betriebssystem Android geschlossen.
- Link

—

E-Book-Tool Calibre: Codeschmuggel durch kritische Sicherheitslücke möglich
Durch eine kritische Sicherheitslücke im E-Book-Tool Calibre können nicht angemeldete Angreifer Code einschleusen. Ein Update dichtet das Leck ab.
- Link

—

Kritische Sicherheitslücke bedroht Unternehmenssoftware Apache OFBiz
Angreifer können Systeme mit Apache OFBiz attackieren und eigenen Code ausführen. Eine dagegen abgesicherte Version steht zum Download bereit.
- Link

—

Unbefugte Zugriffe auf IT-Managementlösung Aruba ClearPass möglich
Die Entwickler von HPE Aruba Networking haben in ClearPass Policy Manager unter anderem eine kritische Sicherheitslücke geschlossen.
- Link

—

Kritische Sicherheitslücke bedroht Google Chrome
Angreifer können an mehreren Schwachstellen in Chrome ansetzen, um PCs zu kompromittieren.
- Link

—

Keine Sicherheitsupdates in Sicht: Avast Free Antivirus ist verwundbar
Sicherheitsforscher warnen vor Schwachstellen in Avast Free Antivirus und raten aufgrund fehlender Patches von einer Nutzung ab.
- Link

—

Jetzt patchen! Ransomware-Attacken auf VMware ESXi-Server beobachtet
Sicherheitsforscher warnen vor laufenden Attacken auf Systeme mit ESXi-Hypervisor. Darüber

gelangen Erpressungstrojaner auf Computer.
- Link

—

Selenium Grid: Unsichere Standardkonfiguration lässt Krypto-Miner passieren

Das Framework für automatisierte Softwaretests Selenium Grid ist in den Standardeinstellungen verwundbar. Das nutzen Angreifer derzeit aus.
- Link

—

Angreifer nutzen Schadcode-Lücke in Acronis Cyber Infrastructure aus

In mehreren aktualisierten Versionen von Acronis Cyber Infrastructure haben die Entwickler eine kritische Lücke geschlossen.
- 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-2023-7028	0.903160000	0.988660000	Link
CVE-2023-6895	0.922010000	0.990020000	Link
CVE-2023-6553	0.925190000	0.990400000	Link
CVE-2023-5360	0.903980000	0.988720000	Link
CVE-2023-52251	0.940460000	0.991990000	Link
CVE-2023-4966	0.971280000	0.998270000	Link
CVE-2023-49103	0.962110000	0.995540000	Link
CVE-2023-48795	0.964660000	0.996150000	Link
CVE-2023-47246	0.957550000	0.994730000	Link
CVE-2023-46805	0.936080000	0.991490000	Link
CVE-2023-46747	0.972730000	0.998800000	Link
CVE-2023-46604	0.961790000	0.995480000	Link
CVE-2023-4542	0.928310000	0.990680000	Link
CVE-2023-43208	0.965360000	0.996420000	Link
CVE-2023-43177	0.965600000	0.996490000	Link
CVE-2023-42793	0.970370000	0.997900000	Link
CVE-2023-41265	0.911110000	0.989200000	Link
CVE-2023-39143	0.941900000	0.992180000	Link
CVE-2023-38646	0.906610000	0.988900000	Link
CVE-2023-38205	0.947910000	0.993080000	Link
CVE-2023-38203	0.966410000	0.996670000	Link
CVE-2023-38035	0.974680000	0.999710000	Link
CVE-2023-36845	0.964250000	0.996070000	Link
CVE-2023-3519	0.965340000	0.996400000	Link
CVE-2023-35082	0.968030000	0.997170000	Link
CVE-2023-35078	0.970390000	0.997910000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34993	0.972640000	0.998770000	Link
CVE-2023-34960	0.936550000	0.991550000	Link
CVE-2023-34634	0.930910000	0.990990000	Link
CVE-2023-34468	0.906650000	0.988900000	Link
CVE-2023-34362	0.969450000	0.997590000	Link
CVE-2023-34039	0.944910000	0.992640000	Link
CVE-2023-3368	0.935570000	0.991430000	Link
CVE-2023-33246	0.972140000	0.998570000	Link
CVE-2023-32315	0.970550000	0.997980000	Link
CVE-2023-30625	0.948260000	0.993150000	Link
CVE-2023-30013	0.962790000	0.995700000	Link
CVE-2023-29300	0.968930000	0.997410000	Link
CVE-2023-29298	0.943640000	0.992440000	Link
CVE-2023-28432	0.906190000	0.988850000	Link
CVE-2023-28343	0.923780000	0.990230000	Link
CVE-2023-28121	0.909500000	0.989080000	Link
CVE-2023-27524	0.970600000	0.998000000	Link
CVE-2023-27372	0.973190000	0.999000000	Link
CVE-2023-27350	0.969960000	0.997770000	Link
CVE-2023-26469	0.956500000	0.994570000	Link
CVE-2023-26360	0.965230000	0.996350000	Link
CVE-2023-26035	0.967950000	0.997150000	Link
CVE-2023-25717	0.954090000	0.994100000	Link
CVE-2023-25194	0.968820000	0.997390000	Link
CVE-2023-2479	0.963740000	0.995930000	Link
CVE-2023-24489	0.973540000	0.999140000	Link
CVE-2023-23752	0.956380000	0.994550000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23333	0.958950000	0.994940000	Link
CVE-2023-22527	0.968290000	0.997230000	Link
CVE-2023-22518	0.964890000	0.996200000	Link
CVE-2023-22515	0.973730000	0.999230000	Link
CVE-2023-21839	0.957210000	0.994670000	Link
CVE-2023-21554	0.952830000	0.993860000	Link
CVE-2023-20887	0.970670000	0.998020000	Link
CVE-2023-1671	0.962480000	0.995610000	Link
CVE-2023-0669	0.969440000	0.997570000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 06 Aug 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht nicht spezifizierten Angriff

Ein Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Tue, 06 Aug 2024

[UPDATE] [hoch] Python: Mehrere Schwachstellen

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

- Link

—

Tue, 06 Aug 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service zu verursachen.

- Link

—

Tue, 06 Aug 2024

[UPDATE] [hoch] SMTP Implementierungen: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen SMTP Implementierungen ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Tue, 06 Aug 2024

[UPDATE] [hoch] GNU Emacs: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in GNU Emacs ausnutzen, um beliebigen Programmcode auszuführen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Tue, 06 Aug 2024

[UPDATE] [hoch] less: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in less ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Tue, 06 Aug 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

—

Tue, 06 Aug 2024

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

Ein Angreifer kann eine Schwachstelle in GNU libc ausnutzen, um einen Denial-of-Service-Zustand zu verursachen, Code auszuführen oder seine Privilegien zu erweitern.

- Link

—

Tue, 06 Aug 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um Sicherheitsvorkehrungen zu umgehen und um Dateien zu manipulieren.

- Link

—

Tue, 06 Aug 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, 06 Aug 2024

[UPDATE] [hoch] Ghostscript: Mehrere Schwachstellen

Ein entfernter anonymer oder ein lokaler Angreifer kann mehrere Schwachstellen in Ghostscript ausnutzen, um Informationen offenzulegen oder beliebigen Code auszuführen.

- Link

—

Tue, 06 Aug 2024

[UPDATE] [hoch] RADIUS: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein lokaler Angreifer kann eine Schwachstelle im RADIUS Protokoll ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Tue, 06 Aug 2024

[NEU] [hoch] Android Patchday August 2024

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um seine Privilegien zu erweitern, einen Denial-of-Service-Zustand zu erzeugen, beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen

- Link

—

Tue, 06 Aug 2024

[NEU] [hoch] Kibana: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Tue, 06 Aug 2024

[NEU] [hoch] JFrog Artifactory: Schwachstelle ermöglicht Manipulation von Dateien

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in JFrog Artifactory ausnutzen, um Dateien zu manipulieren.

- Link

—

Tue, 06 Aug 2024

[NEU] [hoch] Foxit PDF Editor: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Foxit PDF Editor ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu erzeugen und vertrauliche Informationen preiszugeben.

- Link

—

Tue, 06 Aug 2024

[UPDATE] [hoch] ImageMagick: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit Benutzerrechten

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in ImageMagick ausnutzen, um beliebigen Programmcode mit Benutzerrechten auszuführen.

- Link

—

Tue, 06 Aug 2024

[UPDATE] [hoch] ImageMagick: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Tue, 06 Aug 2024

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

Ein Angreifer kann eine Schwachstelle in OpenSSL ausnutzen, um einen Denial of Service Angriff durchzuführen oder unbekannte Auswirkungen zu verursachen.

- Link

—

Tue, 06 Aug 2024

[UPDATE] [hoch] Intel Prozessoren: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in verschiedenen Intel Prozessoren ausnutzen, um einen Denial of Service Angriff durchzuführen, beliebigen Programmcode auszuführen, seine Privilegien zu erweitern oder Informationen offenzulegen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/6/2024	[CBL Mariner 2.0 Security Update: emacs (CVE-2024-39331)]	critical
8/6/2024	[Amazon Linux 2023 : tpm2-tools (ALAS2023-2024-693)]	critical
8/6/2024	[Amazon Linux 2023 : openssl, openssl-devel, openssl-libs (ALAS2023-2024-677)]	critical
8/6/2024	[CBL Mariner 2.0 Security Update: qemu (CVE-2021-3929)]	high
8/6/2024	[CBL Mariner 2.0 Security Update: qemu / qemu-kvm (CVE-2021-4207)]	high
8/6/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-39277)]	high
8/6/2024	[CBL Mariner 2.0 Security Update: qemu (CVE-2022-26353)]	high
8/6/2024	[CBL Mariner 2.0 Security Update: python3 (CVE-2024-0397)]	high
8/6/2024	[CBL Mariner 2.0 Security Update: terraform (CVE-2024-6257)]	high
8/6/2024	[CBL Mariner 2.0 Security Update: qemu / qemu-kvm (CVE-2022-2962)]	high
8/6/2024	[CBL Mariner 2.0 Security Update: gtk2 / gtk3 (CVE-2024-6655)]	high
8/6/2024	[CBL Mariner 2.0 Security Update: qemu / qemu-kvm (CVE-2021-3750)]	high
8/6/2024	[CBL Mariner 2.0 Security Update: curl (CVE-2024-2398)]	high
8/6/2024	[Debian dsa-5738 : openjdk-17-dbg - security update]	high
8/6/2024	[Debian dsa-5739 : eapoltest - security update]	high
8/6/2024	[Amazon Linux 2023 : ghostscript, ghostscript-gtk, ghostscript-tools-dvipdf (ALAS2023-2024-692)]	high
8/6/2024	[Amazon Linux 2023 : aspnetcore-runtime-6.0, aspnetcore-targeting-pack-6.0, dotnet (ALAS2023-2024-685)]	high
8/6/2024	[Amazon Linux 2023 : gtk3, gtk3-devel, gtk3-immodule-xim (ALAS2023-2024-675)]	high
8/6/2024	[Amazon Linux 2023 : httpd, httpd-core, httpd-devel (ALAS2023-2024-681)]	high

Datum	Schwachstelle	Bewertung
8/6/2024	[Amazon Linux 2023 : python3-setuptools, python3-setuptools-wheel (ALAS2023-2024-676)]	high
8/6/2024	[Amazon Linux 2023 : python3, python3-devel, python3-idle (ALAS2023-2024-699)]	high
8/6/2024	[Amazon Linux 2023 : containerd, containerd-stress (ALAS2023-2024-697)]	high
8/6/2024	[Amazon Linux 2023 : rapidjson-devel (ALAS2023-2024-684)]	high
8/6/2024	[Amazon Linux 2023 : kernel (ALAS2023-2024-696)]	high
8/6/2024	[Amazon Linux 2023 : aspnetcore-runtime-8.0, aspnetcore-runtime-dbg-8.0, aspnetcore-targeting-pack-8.0 (ALAS2023-2024-686)]	high
8/6/2024	[Amazon Linux 2023 : kernel (ALAS2023-2024-695)]	high
8/6/2024	[Amazon Linux 2023 : krb5-devel, krb5-libs, krb5-pkinit (ALAS2023-2024-688)]	high
8/6/2024	[Amazon Linux 2023 : bind, bind-chroot, bind-devel (ALAS2023-2024-680)]	high
8/6/2024	[Amazon Linux 2023 : bpftool, kernel, kernel-devel (ALAS2023-2024-679)]	high
8/6/2024	[Amazon Linux 2023 : ca-certificates (ALAS2023-2024-682)]	high
8/6/2024	[Amazon Linux 2023 : libsndfile, libsndfile-devel, libsndfile-utils (ALAS2023-2024-701)]	high
8/6/2024	[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Django vulnerabilities (USN-6946-1)]	high
8/6/2024	[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : wpa_supplicant and hostapd vulnerability (USN-6945-1)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Tue, 06 Aug 2024

Korenix JetPort Series 1.2 Command Injection / Insufficient Authentication

Korenix JetPort Series version 1.2 suffers from insufficient authentication, command injection, and plaintext communication vulnerabilities.

- Link

—

” “Tue, 06 Aug 2024

Microweber 2.0.15 Cross Site Scripting

Microweber version 1.0 suffers from a cross site scripting vulnerability in the search functionality. Original discovery of cross site scripting in this version is attributed to tmrswrr in June of 2024.

- Link

—

” “Tue, 06 Aug 2024

eduAuthorities 1.0 SQL Injection

eduAuthorities version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Tue, 06 Aug 2024

Concert Ticket Reservation System 1.0 SQL Injection

Concert Ticket Reservation System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Tue, 06 Aug 2024

Computer Laboratory Management System 1.0 Insecure Settings

Computer Laboratory Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Tue, 06 Aug 2024

Codeprojects E-Commerce 1.0 Cross Site Scripting

Codeprojects E-Commerce version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Tue, 06 Aug 2024

Blog Site 1.0 Cross Site Scripting

Blog Site version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 05 Aug 2024

Linux DRM drm_file_update_pid() Race Condition / Use-After-Free

Linux DRM has drm_file_update_pid() call to get_pid() too late, which creates a race condition that can lead to use-after-free issue of a struct pid.

- Link

—

” “Mon, 05 Aug 2024

Online Shopping Portal Project 2.0 SQL Injection

Online Shopping Portal Project version 2.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 05 Aug 2024

Dolphin 7.4.2 Blind SQL Injection

Dolphin version 7.4.2 suffers from a remote blind SQL injection vulnerability.

- Link

—

” “Mon, 05 Aug 2024

Ivanti ADC 9.9 Authentication Bypass

Ivanti ADC version 9.9 suffers from an authentication bypass vulnerability.

- Link

—

” “Mon, 05 Aug 2024

Genexus Protection Server 9.7.2.10 Unquoted Service Path

Genexus Protection Server version 9.7.2.10 suffers from an unquoted service path vulnerability.

- Link

—

” “Mon, 05 Aug 2024

Devika 1 Path Traversal

Devika version 1 suffers from a path traversal vulnerability.

- Link

—

” “Mon, 05 Aug 2024

e107 2.3.3 Cross Site Scripting

e107 version 2.3.3 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 05 Aug 2024

Codeprojects E-Commerce 1.0 Insecure Settings

Codeprojects E-Commerce version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 05 Aug 2024

Blog Site 1.0 SQL Injection

Blog Site version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Mon, 05 Aug 2024

Best Courier Management System 1.0 SQL Injection

Best Courier Management System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Mon, 05 Aug 2024

Appointment Scheduler 4.0 Insecure Direct Object Reference

Appointment Scheduler version 4.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Fri, 02 Aug 2024

Packet Storm New Exploits For July, 2024

This archive contains all of the 105 exploits added to Packet Storm in July, 2024.

- Link

—

” “Fri, 02 Aug 2024

Tourism Management System 2.0 Cross Site Scripting

Tourism Management System version 2.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Fri, 02 Aug 2024

Computer Laboratory Management System 1.0 Privilege Escalation

Computer Laboratory Management System version 1.0 suffers from an incorrect access control that

allows for privilege escalation.
- Link
—
” “Fri, 02 Aug 2024
Leads Manager Tool SQL Injection / Cross Site Scripting
Leads Manager Tool suffers from remote SQL injection and cross site scripting vulnerabilities.
- Link
—
” “Fri, 02 Aug 2024
ReadyMade Unilevel Ecommerce MLM Blind SQL Injection / Cross Site Scripting
Readymade Unilevel Ecommerce MLM suffers from remote blind SQL injection and cross site scripting vulnerabilities. These issues affected the version released as late as March 15, 2024.
- Link
—
” “Fri, 02 Aug 2024
Appointment Scheduler 3.0 Insecure Direct Object Reference
Appointment Scheduler version 3.0 suffers from an insecure direct object reference vulnerability.
- Link
—
” “Fri, 02 Aug 2024
AccPack Cop 1.0 Cross Site Request Forgery
AccPack Cop version 1.0 suffers from a cross site request forgery vulnerability.
- Link
—
”

4.2 0-Days der letzten 5 Tage

“Tue, 06 Aug 2024
ZDI-24-1101: Apple macOS Metal Framework KTX Image Parsing Out-Of-Bounds Read Information Disclosure Vulnerability
- Link
—
” “Tue, 06 Aug 2024
ZDI-24-1100: SMARTBEAR SoapUI unpackageAll Directory Traversal Remote Code Execution Vulnerability
- Link
—

” “Tue, 06 Aug 2024

ZDI-24-1099: Apache OFBiz resolveURI Authentication Bypass Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1098: (0Day) Microsoft Windows Error Reporting Service Missing Authorization Arbitrary Process Termination Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1097: (0Day) Microsoft GitHub Dev-Containers Improper Privilege Management Privilege Escalation Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1096: (0Day) Microsoft Office Visio EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1095: (0Day) Microsoft Office Visio DXF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1094: (0Day) Microsoft Office Visio EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1093: (0Day) Microsoft Office Visio EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1092: (0Day) Microsoft Office Visio DXF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1091: (0Day) Microsoft Windows DirectComposition Out-Of-Bounds Read Denial-of-Service Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1090: (0Day) Microsoft Windows DirectComposition Null Pointer Dereference Denial-of-Service Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1089: (0Day) Microsoft Office Visio DXF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1088: (0Day) Microsoft 3D Viewer GLB File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1087: (0Day) oFono SMS Decoder Stack-based Buffer Overflow Privilege Escalation Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1086: (0Day) oFono SimToolKit Heap-based Buffer Overflow Privilege Escalation Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1085: (0Day) oFono SimToolKit Heap-based Buffer Overflow Privilege Escalation Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1084: (0Day) oFono SimToolKit Heap-based Buffer Overflow Privilege Escalation Vul-

nerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1083: (0Day) oFono SimToolKit Heap-based Buffer Overflow Privilege Escalation Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1082: (0Day) (Pwn2Own) oFono AT CMGR Command Uninitialized Variable Information Disclosure Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1081: (0Day) (Pwn2Own) oFono AT CMT Command Uninitialized Variable Information Disclosure Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1080: (0Day) (Pwn2Own) oFono AT CMGL Command Uninitialized Variable Information Disclosure Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1079: (0Day) (Pwn2Own) oFono CUSD Stack-based Buffer Overflow Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1078: (0Day) (Pwn2Own) oFono CUSD AT Command Stack-based Buffer Overflow Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1077: (0Day) (Pwn2Own) oFono QMI SMS Handling Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1076: Microsoft Windows Menu DC Color Space Use-After-Free Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1075: Microsoft PowerShell Reference for Office Products officedocs-cdn Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1074: Microsoft PowerShell Gallery psg-prod-centralus Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1073: Microsoft Azure uAMQP azure-iot-sdks-ci Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1072: Microsoft CameraTraps cameratracrsppftkje Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1071: Microsoft Azure GPT ALE palantirdemoacr Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1070: Microsoft Partner Resources openhacks Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1069: Microsoft Technical Case Studies athena-dashboard Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1068: Microsoft Azure ML.NET Samples mlnetfilestorage Uncontrolled Search Path Element Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1067: Microsoft Azure CollectSFData docs-analytics-eus Uncontrolled Search Path Element Impersonation Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1066: Microsoft Azure DataStoriesSamples machinelearningdatasets Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1065: Microsoft Azure Availability Monitor for Kafka esnewdeveastdockerregistry Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1064: Microsoft AirSim airsimci Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1063: Microsoft Reactor Workshops reactorworkshops Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1062: Microsoft Fluid Framework prague Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1061: Microsoft What The Hack docsmsftpdfs Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1060: Microsoft Azure Aztack aztack1528763526 Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1059: Microsoft Azure Linux Automation konkaciwestus1 Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1058: Microsoft Azure NodeJS LogPoint logpointsassets Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1057: Trimble SketchUp Pro SKP File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1056: Trimble SketchUp SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1055: Trimble SketchUp SKP File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1054: Trimble SketchUp Viewer SKP File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—
”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Wieder mal die Lieferkette: polyfill.io wird verkauft, spielt Schadcode aus.

Zum Youtube Video

6 Cyberangriffe: (Aug)

Datum	Opfer	Land	Information
2024-08-04	RMN-Grand Palais	[FRA]	Link
2024-08-03	Xtrim	[ECU]	Link

7 Ransomware-Erpressungen: (Aug)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-06	[msprocuradores.es]	madliberator	Link
2024-08-06	[www.carri.com]	alphalocker	Link
2024-08-06	[www.consorzioinnova.it]	alphalocker	Link
2024-08-06	[goftac.com/ firsttx.com First Texas Alliance Corp (FTAC)]	alphalocker	Link
2024-08-06	[biw-burger.de]	alphalocker	Link
2024-08-06	[www.sobha.com]	ransomhub	Link
2024-08-06	[Alternate Energy]	play	Link
2024-08-06	[True Blue Environmental]	play	Link
2024-08-06	[Granit Design]	play	Link
2024-08-06	[KinetX]	play	Link
2024-08-06	[Omni Family Health]	hunters	Link
2024-08-06	[IOI Corporation Berhad]	fog	Link
2024-08-06	[Ziba Design]	fog	Link
2024-08-06	[Casco Antiguo]	hunters	Link
2024-08-06	[Fractalia Group]	hunters	Link
2024-08-06	[Banx Systems]	meow	Link
2024-08-05	[Silipos]	cicada3301	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-04	[kierlcpa.com]	lockbit3	Link
2024-08-05	[Square One Coating Systems]	cicada3301	Link
2024-08-05	[Hi-P International]	fog	Link
2024-08-05	[Zon Beachside zonbeachside.com]	dispossessor	Link
2024-08-05	[HP Distribution]	incransom	Link
2024-08-05	[exco-solutions.com]	cactus	Link
2024-08-05	[Maryville Academy]	rhysida	Link
2024-08-04	[notariusze.waw.pl]	killsec	Link
2024-08-04	[Ranney School]	rhysida	Link
2024-08-03	[nursing.com]	ransomexx	Link
2024-08-03	[Bettis Asphalt]	blacksuit	Link
2024-08-03	[fcl.crs]	lockbit3	Link
2024-08-03	[CPA Tax Solutions]	meow	Link
2024-08-03	[LRN]	hunters	Link
2024-08-03	[aikenhousing.org]	blacksuit	Link
2024-08-02	[David E Shambach Architect]	dragonforce	Link
2024-08-02	[Hayes Beer Distributing]	dragonforce	Link
2024-08-02	[Jangho Group]	hunters	Link
2024-08-02	[Khandelwal Laboratories Pvt]	hunters	Link
2024-08-02	[retaildatallc.com]	ransomhub	Link
2024-08-02	[WPG Holdings]	meow	Link
2024-08-02	[National Beverage]	meow	Link
2024-08-02	[PeoplesHR]	meow	Link
2024-08-02	[Dometic Group]	meow	Link
2024-08-02	[Remitano]	meow	Link
2024-08-02	[Premier Equities]	meow	Link
2024-08-01	[Kemlon Products & Development Co Inc]	spacebears	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-02	[q-cells.de]	abyss	Link
2024-08-02	[coinbv.nl]	madliberator	Link
2024-08-01	[Valley Bulk]	cicada3301	Link
2024-08-01	[ENEA Italy]	hunters	Link
2024-08-01	[mcdowallaffleck.com.au]	ransomhub	Link
2024-08-01	[effinghamschools.com]	ransomhub	Link
2024-08-01	[warrendale-wagyu.co.uk]	darkvault	Link
2024-08-01	[Adorna & Guzman Dentistry]	monti	Link
2024-08-01	[Camp Susque]	medusa	Link
2024-08-01	[Ali Gohar]	medusa	Link
2024-08-01	[acsi.org]	blacksuit	Link
2024-08-01	[County Linen UK]	dispossessor	Link
2024-08-01	[TNT Materials tnt-materials.com/]	dispossessor	Link
2024-08-01	[Peñoles]	akira	Link
2024-08-01	[dahlvalve.com]	cactus	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.