Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240709

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

Root- und Backdoor-Lücken in Mufus von Toshiba und Sharp geschlossen
Angreifer können hunderte Multifunktionsdrucker von Toshiba und Sharp ins Visier nehmen. Sicherheitsupdates sind verfügbar.
- Link

—

Mastodon: Sicherheitslücke ermöglicht unbefugten Zugriff auf Posts
Betreiber von Mastodon-Instanzen sollten zügig ihre Serversoftware aktualisieren. Eine hochriskant Lücke erlaubt unbefugten Zugriff auf Posts.
- Link

—

Android: Google schließt teils kritische Lücken am Juli-Patchday
Google hat Updates für Android 12, 12L, 13 und 14 im Rahmen des Juli-Patchdays veröffentlicht. Sie schließen Rechteausweitungs-Lücken.
- Link

—

Update für IBM InfoSphere Information Server dichtet viele Sicherheitslücken ab
IBM hat mehrere Sicherheitswarnungen zum InfoSphere Information Server herausgegeben. Aktualisierte Software korrigiert die Fehler.
- Link

—

Juniper: Notfall-Update für Junos OS auf SRX-Baureihe
Juniper Networks schließt eine als hochriskant eingestufte DoS-Lücke im Juniper OS der SRX-Geräte mit einem Update außer der Reihe.
- Link

—

RegreSSHion: Sicherheitslücke in OpenSSH gibt geduldigen Angreifern Root-Rechte
Wer die alte, neue Lücke im SSH-Server ausnutzen möchte, braucht Sitzfleisch: Bis zur Root-Shell dauert es 8 Stunden. Dafür klappt der Angriff aus der Ferne.
- Link

—

IP-Telefonie: Avaya IP Office stopft kritische Sicherheitslecks
Updates für Avaya IP Office dichten Sicherheitslecks in der Software ab. Angreifer können dadurch Schadcode einschleusen.
- Link

—

Juniper: Kritische Lücke erlaubt Angreifern Übernahme von Session Smart Router

Juniper Networks liefert außerplanmäßige Updates gegen eine kritische Sicherheitslücke in Session Smart Router, -Conductor und WAN Assurance Router.

- Link

—

APT-Angriff auf Fernwartungssoftware? Sicherheitsvorfall bei TeamViewer

Noch ist über das Ausmaß des Angriffs gegen die Fernwartungssoftware nicht viel bekannt - erste Hinweise auf die Urheber deuten auf Profis hin.

- Link

—

Bitte patchen! Security-Update behebt kritische Schwachstelle in GitLab

Eine Reihe von Schwachstellen ermöglichen es in GitLab, CI-Pipelines als anderer User zu starten oder Cross-Site-Scripting über Commit Notes einzuschleusen.

- 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	0.962510000	0.995460000	Link
CVE-2023-6895	0.920390000	0.989650000	Link
CVE-2023-6553	0.934680000	0.991140000	Link
CVE-2023-5360	0.911260000	0.988950000	Link
CVE-2023-52251	0.930900000	0.990750000	Link
CVE-2023-4966	0.971290000	0.998100000	Link
CVE-2023-49103	0.938900000	0.991640000	Link
CVE-2023-48795	0.962520000	0.995470000	Link
CVE-2023-47246	0.953220000	0.993790000	Link
CVE-2023-46805	0.958670000	0.994710000	Link
CVE-2023-46747	0.972630000	0.998610000	Link
CVE-2023-46604	0.963510000	0.995730000	Link
CVE-2023-4542	0.924200000	0.990050000	Link
CVE-2023-43208	0.959520000	0.994880000	Link
CVE-2023-43177	0.962660000	0.995500000	Link
CVE-2023-42793	0.970470000	0.997750000	Link
CVE-2023-41265	0.905890000	0.988570000	Link
CVE-2023-39143	0.940070000	0.991760000	Link
CVE-2023-38646	0.906240000	0.988610000	Link
CVE-2023-38205	0.954590000	0.994040000	Link
CVE-2023-38203	0.968820000	0.997220000	Link
CVE-2023-38146	0.905210000	0.988520000	Link
CVE-2023-38035	0.974610000	0.999610000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.963940000	0.995830000	Link
CVE-2023-3519	0.965360000	0.996230000	Link
CVE-2023-35082	0.967060000	0.996690000	Link
CVE-2023-35078	0.968330000	0.997090000	Link
CVE-2023-34993	0.971260000	0.998090000	Link
CVE-2023-34960	0.927460000	0.990360000	Link
CVE-2023-34634	0.927960000	0.990390000	Link
CVE-2023-34468	0.906650000	0.988630000	Link
CVE-2023-34362	0.969920000	0.997570000	Link
CVE-2023-34039	0.944490000	0.992360000	Link
CVE-2023-3368	0.933870000	0.991070000	Link
CVE-2023-33246	0.972790000	0.998690000	Link
CVE-2023-32315	0.973600000	0.999090000	Link
CVE-2023-30625	0.943100000	0.992130000	Link
CVE-2023-30013	0.962250000	0.995390000	Link
CVE-2023-29300	0.968380000	0.997110000	Link
CVE-2023-29298	0.943170000	0.992150000	Link
CVE-2023-28771	0.902140000	0.988340000	Link
CVE-2023-28343	0.948520000	0.992990000	Link
CVE-2023-28121	0.909760000	0.988840000	Link
CVE-2023-27524	0.970570000	0.997780000	Link
CVE-2023-27372	0.973020000	0.998800000	Link
CVE-2023-27350	0.969800000	0.997540000	Link
CVE-2023-26469	0.935230000	0.991200000	Link
CVE-2023-26360	0.957000000	0.994460000	Link
CVE-2023-26035	0.967100000	0.996710000	Link
CVE-2023-25717	0.956860000	0.994430000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-25194	0.969960000	0.997590000	Link
CVE-2023-2479	0.963760000	0.995790000	Link
CVE-2023-24489	0.973310000	0.998950000	Link
CVE-2023-23752	0.954250000	0.993990000	Link
CVE-2023-23397	0.901800000	0.988320000	Link
CVE-2023-23333	0.964220000	0.995880000	Link
CVE-2023-22527	0.970550000	0.997770000	Link
CVE-2023-22518	0.965950000	0.996370000	Link
CVE-2023-22515	0.973330000	0.998960000	Link
CVE-2023-21839	0.956220000	0.994350000	Link
CVE-2023-21554	0.950840000	0.993350000	Link
CVE-2023-20887	0.971080000	0.998000000	Link
CVE-2023-1671	0.964510000	0.995940000	Link
CVE-2023-0669	0.969330000	0.997370000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 08 Jul 2024

[NEU] [hoch] Apache CloudStack: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Apache CloudStack ausnutzen, um beliebigen Code auszuführen oder seine Privilegien zu erweitern.

- Link

—

Mon, 08 Jul 2024

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

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

- Link

—

Mon, 08 Jul 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

—

Mon, 08 Jul 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen ermöglichen Manipulation von Dateien

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um Dateien zu manipulieren.

- Link

—

Mon, 08 Jul 2024

[UPDATE] [hoch] Mozilla Firefox und Firefox ESR: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Firefox ESR ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 08 Jul 2024

[UPDATE] [hoch] Microsoft Windows: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Windows 10, Microsoft Windows 11, Microsoft Windows Server, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019 und Microsoft Windows Server 2022 ausnutzen, um seine Privilegien zu erweitern, beliebigen Programmcode auszuführen, beliebigen Programmcode mit Administratorrechten auszuführen, Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen, einen Denial of Service Zustand herbeizuführen oder Dateien zu manipulieren

- Link

—

Mon, 08 Jul 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

—

Mon, 08 Jul 2024

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

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen oder Daten zu manipulieren.

- Link

—

Mon, 08 Jul 2024

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

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

- Link

—

Mon, 08 Jul 2024

[UPDATE] [hoch] OpenSSH: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in OpenSSH ausnutzen, um beliebigen Programmcode mit root Rechten auszuführen.

- Link

—

Fri, 05 Jul 2024

[UPDATE] [hoch] BusyBox: Mehrere Schwachstellen

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in BusyBox ausnutzen, um einen Denial of Service Angriff durchzuführen, Informationen offenzulegen oder beliebigen Code auszuführen.

- Link

—

Fri, 05 Jul 2024

[UPDATE] [hoch] docker: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Docker ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder Dateien zu manipulieren.

- Link

—

Fri, 05 Jul 2024

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

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

- Link

—

Fri, 05 Jul 2024

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

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

- Link

—

Fri, 05 Jul 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

—

Fri, 05 Jul 2024

[UPDATE] [hoch] PuTTY: Schwachstelle ermöglicht Erlangen des privaten Schlüssels

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PuTTY und Anwendungen, die PuTTY nutzen, wie z.B. FileZilla, WinSCP und TortoiseGit ausnutzen, um bei 521-bit ECDSA den privaten Schlüssel des Nutzers zu erlangen.

- Link

—

Thu, 04 Jul 2024

[UPDATE] [hoch] Google Android: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um seine Privilegien zu erhöhen, vertrauliche Informationen offenzulegen, beliebigen Code zur Ausführung zu bringen und einen Denial-of-Service-Zustand auszulösen.

- Link

—

Thu, 04 Jul 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

—

Thu, 04 Jul 2024

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

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

- Link

—

Thu, 04 Jul 2024

[UPDATE] [hoch] Apple iOS: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
7/8/2024	[RHEL 9 : kernel (RHSA-2024:4349)]	critical
7/8/2024	[RHEL 8 : postgresql-jdbc (RHSA-2024:4375)]	critical
7/8/2024	[RHEL 9 : git (RHSA-2024:4368)]	critical
7/8/2024	[Node.js 18.x < 18.20.4 / 20.x < 20.15.1 / 22.x < 22.4.1 Multiple Vulnerabilities (Monday, July 8, 2024 Security Releases).]	critical
7/8/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Apache HTTP Server vulnerabilities (USN-6885-1)]	critical
7/5/2024	[Juniper SSR Security Bypass (JSA83126)]	critical
7/5/2024	[GLSA-202407-18 : Stellarium: Arbitrary File Write]	critical
7/8/2024	[RHEL 8 : nodejs:16 (RHSA-2024:4353)]	high
7/8/2024	[RHEL 8 : kernel-rt (RHSA-2024:4352)]	high
7/8/2024	[Tenable.ad < 3.59.5 Multiple Vulnerabilities (TNS-2024-11)]	high
7/8/2024	[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Tomcat vulnerability (USN-6880-1)]	high
7/8/2024	[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS : Exim vulnerability (USN-6881-1)]	high
7/8/2024	[RHEL 9 : buildah (RHSA-2024:4371)]	high
7/8/2024	[RHEL 8 : pki-core (RHSA-2024:4367)]	high

Datum	Schwachstelle	Bewertung
7/8/2024	[RHEL 8 : virt:rhel and virt-devel:rhel (RHSA-2024:4372)]	high
7/8/2024	[RHEL 8 : virt:rhel and virt-devel:rhel (RHSA-2024:4373)]	high
7/8/2024	[RHEL 8 : virt:rhel and virt-devel:rhel (RHSA-2024:4374)]	high
7/8/2024	[RHEL 8 : python3 (RHSA-2024:4370)]	high
7/8/2024	[RHEL 9 : gvisor-tap-vsock (RHSA-2024:4379)]	high
7/8/2024	[RHEL 9 : podman (RHSA-2024:4378)]	high
7/8/2024	[RHEL 8 : less (RHSA-2024:4366)]	high
7/8/2024	[RHEL 8 : less (RHSA-2024:4369)]	high
7/8/2024	[FreeBSD : traefik – Bypassing IP allow-lists via HTTP/3 early data requests (767dfb2d-3c9e-11ef-a829-5404a68ad561)]	high
7/8/2024	[RHEL 9 : openssh (RHSA-2024:4389)]	high
7/8/2024	[RHEL 8 / 9 : Red Hat JBoss Enterprise Application Platform 8.0 (RHSA-2024:4390)]	high
7/8/2024	[Oracle Linux 9 : gvisor-tap-vsock (ELSA-2024-4379)]	high
7/8/2024	[Oracle Linux 9 : buildah (ELSA-2024-4371)]	high
7/8/2024	[Oracle Linux 9 : podman (ELSA-2024-4378)]	high
7/8/2024	[IBM WebSphere Application Server 8.5.x < 8.5.5.26 / 9.x < 9.0.5.21 RCE (7159825)]	high
7/7/2024	[Fedora 40 : yt-dlp (2024-0ba1c1a435)]	high
7/7/2024	[openSUSE 15 Security Update : opera (openSUSE-SU-2024:0187-1)]	high
7/6/2024	[Debian dsa-5726 : krb5-admin-server - security update]	high
7/6/2024	[SUSE SLES15 Security Update : krb5 (SUSE-SU-2024:2305-1)]	high
7/6/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : krb5 (SUSE-SU-2024:2307-1)]	high
7/6/2024	[GLSA-202407-22 : Mozilla Firefox: Multiple Vulnerabilities]	high
7/6/2024	[GLSA-202407-20 : KDE Plasma Workspaces: Privilege Escalation]	high

Datum	Schwachstelle	Bewertung
7/6/2024	[GLSA-202407-21 : X.Org X11 library: Multiple Vulnerabilities]	high
7/6/2024	[GLSA-202407-19 : Mozilla Thunderbird: Multiple Vulnerabilities]	high
7/5/2024	[RHEL 9 : openssh (RHSA-2024:4340)]	high
7/5/2024	[AlmaLinux 9 : openssh (ALSA-2024:4312)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Mon, 08 Jul 2024

WordPress Poll 2.3.6 SQL Injection

WordPress Poll plugin version 2.3.6 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 08 Jul 2024

VMWare Aria Operations For Networks Command Injection

VMWare Aria Operations for Networks (vRealize Network Insight) is vulnerable to command injection when accepting user input through the Apache Thrift RPC interface. This is a proof of concept exploit.

- Link

—

” “Mon, 08 Jul 2024

Veeam Backup Enterprise Manager Authentication Bypass

Veeam Backup Enterprise Manager authentication bypass proof of concept exploit. Versions prior to 12.1.2.172 are vulnerable.

- Link

—

” “Mon, 08 Jul 2024

Veeam Recovery Orchestrator Authentication Bypass

Veeam Recovery Orchestrator authentication bypass proof of concept exploit.

- Link

—

” “Mon, 08 Jul 2024

Telerik Report Server Deserialization / Authentication Bypass

Telerik Report Server deserialization and authentication bypass exploit chain that makes use of the vulnerabilities noted in CVE-2024-4358 and CVE-2024-1800.

- Link

—

” “Mon, 08 Jul 2024

Progress WhatsUp Gold WriteDatafile Unauthenticated Remote Code Execution

Progress WhatsUp Gold WriteDatafile unauthenticated remote code execution proof of concept exploit.

- Link

—

” “Mon, 08 Jul 2024

Progress WhatsUp Gold GetFileWithoutZip Unauthenticated Remote Code Execution

Progress WhatsUp Gold GetFileWithoutZip unauthenticated remote code execution proof of concept exploit.

- Link

—

” “Mon, 08 Jul 2024

Progress WhatsUp Gold SetAdminPassword Privilege Escalation

Progress WhatsUp Gold SetAdminPassword local privilege escalation proof of concept exploit.

- Link

—

” “Mon, 08 Jul 2024

ResidenceCMS 2.10.1 Cross Site Scripting

ResidenceCMS versions 2.10.1 and below suffer from a persistent cross site scripting vulnerability.

- Link

—

” “Mon, 08 Jul 2024

PMS 2024 1.0 SQL Injection

PMS 2024 version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 08 Jul 2024

Simple Online Banking System 1.0 SQL Injection

Simple Online Banking System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Mon, 08 Jul 2024

Microsoft Office 365 Remote Code Execution

Microsoft Office 365 appears susceptible to macro code execution that can result in remote code execution.

- Link

—

” “Fri, 05 Jul 2024

WordPress Video Gallery - YouTube Gallery And Vimeo Gallery 2.3.6 SQL Injection

WordPress Video Gallery - YouTube Gallery And Vimeo Gallery version 2.3.6 suffers from a remote SQL injection vulnerability.

- Link

—

” “Fri, 05 Jul 2024

Cinema Booking System 1.0 SQL Injection / Cross Site Request Forgery

Cinema Booking System version 1.0 suffers from remote SQL injection and cross site request forgery vulnerabilities.

- Link

—

” “Thu, 04 Jul 2024

Helmholz Industrial Router REX100 / MBConnectline mbNET.mini 2.2.11 Command Injection

Helmholz Industrial Router REX100 and MBConnectline mbNET.mini versions 2.2.11 and below suffer from a command injection vulnerability.

- Link

—

” “Thu, 04 Jul 2024

Toshiba Multi-Function Printers 40 Vulnerabilities

103 models of Toshiba Multi-Function Printers (MFP) are vulnerable to 40 different vulnerabilities including remote code execution, local privilege escalation, xml injection, and more.

- Link

—

” “Thu, 04 Jul 2024

Zyxel parse_config.py Command Injection

This Metasploit module exploits vulnerabilities in multiple Zyxel devices including the VPN, USG and APT series. The affected firmware versions depend on the device module, see this module’s documentation for more details.

- Link

—

” “Thu, 04 Jul 2024

Sharp Multi-Function Printer 18 Vulnerabilities

308 different models of Sharp Multi-Function Printers (MFP) are vulnerable to 18 different vulnerabilities including remote code execution, local file inclusion, credential disclosure, and more.

- Link

—

” “Thu, 04 Jul 2024

SoftMaker Office / FreeOffice Local Privilege Escalation

SoftMaker Office and FreeOffice suffer from a local privilege escalation vulnerability via the MSI installer. Vulnerable versions include SoftMaker Office 2024 / NX before revision 1214, FreeOffice 2021 Revision 1068, and FreeOffice 2024 before revision 1215.

- Link

—

” “Thu, 04 Jul 2024

WordPress Photo Gallery 1.8.26 Cross Site Scripting

WordPress Photo Gallery plugin version 1.8.26 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Thu, 04 Jul 2024

Siemens CP-8000 / CP-8021 / CP8-022 / CP-8031 / CP-8050 / SICORE Buffer Overread / Escalation

Siemens CP-8000, CP-8021, CP8-022, CP-8031, CP-8050, and SICORE products suffer from buffer overread, privilege escalation, and unsafe storage vulnerabilities.

- Link

—

” “Wed, 03 Jul 2024

Deep Sea Electronics DSE855 Remote Authentication Bypass

Deep Sea Electronics DSE855 is vulnerable to configuration disclosure when direct object reference is made to the Backup.bin file using an HTTP GET request. This will enable an attacker to disclose sensitive information and help her in authentication bypass, privilege escalation, and full system access.

- Link

—

” “Tue, 02 Jul 2024

WordPress FooGallery 2.4.16 Cross Site Scripting

WordPress FooGallery plugin version 2.4.16 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 02 Jul 2024

WordPress Gallery 2.3.6 Cross Site Scripting

WordPress Gallery version 2.3.6 suffers from a persistent cross site scripting vulnerability.
- Link
—
” “Tue, 02 Jul 2024
PowerVR Driver Missing Sanitization
The PowerVR driver does not sanitize ZS-Buffer / MSAA scratch firmware addresses.
- Link
—
”

4.2 0-Days der letzten 5 Tage

“Fri, 05 Jul 2024
ZDI-24-897: Trend Micro Apex One modOSCE SQL Injection 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: (Jul)

Datum	Opfer	Land	Information
2024-07-07	Frankfurter University of Applied Sciences (UAS)	[DEU]	Link
2024-07-04	La Ville d'Ans	[BEL]	Link
2024-07-03	E.S.E. Salud Yopal	[COL]	Link
2024-07-03	Florida Department of Health	[USA]	Link
2024-07-02	Hong Kong Institute of Architects	[HKG]	Link
2024-07-02	Apex	[USA]	Link
2024-07-01	Hiap Seng Industries	[SGP]	Link
2024-07-01	Monroe County government	[USA]	Link

7 Ransomware-Erpressungen: (Jul)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-03	[REPLIGEN]	incransom	Link
2024-07-08	[Raffmetal Spa]	dragonforce	Link
2024-07-08	[Allied Industrial Group]	akira	Link
2024-07-08	[Esedra]	akira	Link
2024-07-08	[Federated Co-operatives]	akira	Link
2024-07-02	[Guhring USA]	incransom	Link
2024-07-06	[noab.nl]	lockbit3	Link
2024-07-07	[Strauss Brands]	medusa	Link
2024-07-07	[Harry Perkins Institute of medical research]	medusa	Link
2024-07-07	[Viasat]	medusa	Link
2024-07-07	[Olympus Group]	medusa	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-07	[MYC Media]	rhysida	Link
2024-07-06	[a-g.com 7/10/24 - data publication 38gb (150K)]	blacksuit	Link
2024-07-03	[baiminstitute.org]	ransomhub	Link
2024-07-05	[The Wacks Law Group]	qilin	Link
2024-07-05	[pomalca.com.pe]	qilin	Link
2024-07-05	[Center for Human Capital Innovation (centerforhci.org)]	incransom	Link
2024-07-05	[waupacacounty-wi.gov]	incransom	Link
2024-07-05	[waupaca.wi.us]	incransom	Link
2024-07-04	[ws-stahl.eu]	lockbit3	Link
2024-07-04	[homelandvinyl.com]	lockbit3	Link
2024-07-04	[eicher.in]	lockbit3	Link
2024-07-05	[National Health Laboratory Services]	blacksuit	Link
2024-07-04	[Un Museau]	spacebears	Link
2024-07-03	[Haylem]	spacebears	Link
2024-07-04	[Elyria Foundry]	play	Link
2024-07-04	[Texas Recycling]	play	Link
2024-07-04	[INDA’s]	play	Link
2024-07-04	[Innerspec Technologies]	play	Link
2024-07-04	[Prairie Athletic Club]	play	Link
2024-07-04	[Fareri Associates]	play	Link
2024-07-04	[Island Transportation Corp.]	bianlian	Link
2024-07-04	[Legend Properties, Inc.]	bianlian	Link
2024-07-04	[Transit Mutual Insurance Corporation]	bianlian	Link
2024-07-03	[hcri.edu]	ransomhub	Link
2024-07-04	[Coquitlam Concrete]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-04	[Multisuns Communication]	hunters	Link
2024-07-04	[gerard-perrier.com]	embargo	Link
2024-07-04	[Abileneisd.org]	cloak	Link
2024-07-03	[sequelglobal.com]	darkvault	Link
2024-07-03	[Explomin]	akira	Link
2024-07-03	[Alimac]	akira	Link
2024-07-03	[badel1862.hr]	blackout	Link
2024-07-03	[ramservices.com]	underground	Link
2024-07-03	[foremedia.net]	darkvault	Link
2024-07-03	[www.swcs-inc.com]	ransomhub	Link
2024-07-03	[valleylandtitleco.com]	donutleaks	Link
2024-07-02	[merrymanhouse.org]	lockbit3	Link
2024-07-02	[fairfieldmemorial.org]	lockbit3	Link
2024-07-02	[www.daesangamerica.com]	ransomhub	Link
2024-07-02	[P1 Technologies]	akira	Link
2024-07-02	[Conexus Medstaff]	akira	Link
2024-07-02	[Salton]	akira	Link
2024-07-01	[www.sfmedical.de]	ransomhub	Link
2024-07-02	[WheelerShip]	hunters	Link
2024-07-02	[Grand Rapids Gravel]	dragonforce	Link
2024-07-02	[Franciscan Friars of the Atonement]	dragonforce	Link
2024-07-02	[Elite Fitness]	dragonforce	Link
2024-07-02	[Gray & Adams]	dragonforce	Link
2024-07-02	[Vermont Panurgy]	dragonforce	Link
2024-07-01	[floridahealth.gov]	ransomhub	Link
2024-07-01	[www.nttdata.ro]	ransomhub	Link
2024-07-01	[Super Gardens]	dragonforce	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-01	[Hampden Veterinary Hospital]	dragonforce	Link
2024-07-01	[Indonesia Terkoneksi]	BrainCipher	Link
2024-07-01	[SYNERGY PEANUT]	akira	Link
2024-07-01	[Ethypharm]	underground	Link
2024-07-01	[latinusa.co.id]	lockbit3	Link
2024-07-01	[kbc-zagreb.hr]	lockbit3	Link
2024-07-01	[maxcess-logistics.com]	killsec	Link
2024-07-01	[Independent Education System]	handala	Link
2024-07-01	[Bartlett & Weigle Co. LPA.]	hunters	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.