Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240415

Inhaltsverzeichnis

1 Editorial **2**

2 Security-News **3**
2.1 Heise - Security-Alert . . . 3

3 Sicherheitslücken **4**
3.1 EPSS . . . 4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit . . . 5
3.2 BSI - Warn- und Informationsdienst (WID) . . . 7
3.3 Sicherheitslücken Meldungen von Tenable . . . 11

4 Aktiv ausgenutzte Sicherheitslücken **13**
4.1 Exploits der letzten 5 Tage . . . 13
4.2 0-Days der letzten 5 Tage . . . 17

5 Die Hacks der Woche **18**
5.0.1 Oh wow, this was *very* close: xz-utils was backdoored . . . 18

6 Cyberangriffe: (Apr) **19**

7 Ransomware-Erpressungen: (Apr) **19**

8 Quellen **20**
8.1 Quellenverzeichnis . . . 20

9 Impressum **21**

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

Sicherheitsupdates: Schwachstellen in PHP gefährden Websites
Die PHP-Entwickler haben mehrere Schwachstellen geschlossen. Eine Sicherheitslücke gilt als kritisch.
- Link

—

BSI warnt vor aktiv angegriffener Sicherheitslücke in Palo-Alto-Firewalls
Das BSI warnt vor einer kritischen Sicherheitslücke in Firewalls von Palo Alto Networks. Sie wird bereits attackiert. Angreifer erhalten root-Zugriff.
- Link

—

Sicherheitslücken: Angreifer können Juniper-Netzwerkgeräte lahmlegen
Wichtige Patches schließen mehrere Schwachstellen in Junos OS, die Firewalls, Router und Switches verwundbar machen.
- Link

—

WLAN-Access-Points von TP-Link 15 Minuten lang nach Reboot attackierbar
Zwei TP-Link-WLAN-Access-Points sind unter anderem für DoS-Attacken anfällig. Sicherheitsupdates sind verfügbar.
- Link

—

Google Chrome: Sandbox-Ausbruch durch bestimmte Gesten möglich
Google hat den Chrome-Webbrowser aktualisiert. Angreifer können Sicherheitslücken zum Ausführen von Schadcode missbrauchen.
- Link

—

Befehlsschmuggel: Kritische Lücke in Programmiersprachen unter Windows
BatBadBut heißt eine kritische Befehlsschmuggel-Lücke, die mehrere Programmiersprachen unter Windows betrifft. Abhilfe ist schwer.
- Link

—

Am besten abschalten: Alte NAS-Geräte von D-Link führen Fremdcode aus
Der Hersteller D-Link bietet keine Patches für die veralteten NAS der ShareCenter-Serie mehr an. Betroffene sollten sie vom Internet trennen oder pensionieren.
- Link

—

Patchday Adobe: Schadcode-Attacken auf Experience Manager & Co. möglich

Adobe hat in mehreren Anwendungen kritische Sicherheitslücken geschlossen. Updates sollten zeitnah installiert werden.

- Link

—

Patchday: Angreifer umgehen erneut Sicherheitsfunktion und attackieren Windows

Microsoft hat wichtige Sicherheitsupdates für unter anderem Bitlocker, Office und Windows Defender veröffentlicht. Zwei Lücken nutzen Angreifer bereits aus.

- Link

—

Fortinet liefert Updates: Admin-Cookie-Klau in FortiOS und FortiProxy möglich

In FortiOS und FortiProxy klaffen mehrere Sicherheitslücken. Unter anderem können Angreifer Admin-Cookies klauen und damit Zugriff erlangen.

- 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	0.987500000	Link
CVE-2023-6553	0.916210000	0.988530000	Link
CVE-2023-5360	0.967230000	0.996450000	Link
CVE-2023-4966	0.964860000	0.995700000	Link
CVE-2023-47246	0.934570000	0.990510000	Link
CVE-2023-46805	0.964290000	0.995560000	Link
CVE-2023-46747	0.971350000	0.997860000	Link
CVE-2023-46604	0.972480000	0.998330000	Link
CVE-2023-43177	0.960880000	0.994680000	Link
CVE-2023-42793	0.970710000	0.997570000	Link
CVE-2023-39143	0.942940000	0.991480000	Link
CVE-2023-38646	0.928720000	0.989910000	Link
CVE-2023-38203	0.967010000	0.996390000	Link
CVE-2023-38035	0.973610000	0.998930000	Link
CVE-2023-36845	0.966640000	0.996260000	Link
CVE-2023-3519	0.911860000	0.988240000	Link
CVE-2023-35082	0.947410000	0.992270000	Link
CVE-2023-35078	0.965840000	0.996040000	Link
CVE-2023-34993	0.944980000	0.991940000	Link
CVE-2023-34960	0.938540000	0.990950000	Link
CVE-2023-34634	0.925600000	0.989570000	Link
CVE-2023-34362	0.960290000	0.994520000	Link
CVE-2023-34039	0.907130000	0.987850000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3368	0.918440000	0.988770000	Link
CVE-2023-33246	0.972820000	0.998500000	Link
CVE-2023-32315	0.973670000	0.998960000	Link
CVE-2023-32235	0.911650000	0.988200000	Link
CVE-2023-30625	0.948330000	0.992440000	Link
CVE-2023-30013	0.956380000	0.993820000	Link
CVE-2023-29300	0.970480000	0.997460000	Link
CVE-2023-29298	0.936290000	0.990710000	Link
CVE-2023-28771	0.921620000	0.989040000	Link
CVE-2023-28432	0.943220000	0.991550000	Link
CVE-2023-28121	0.943690000	0.991630000	Link
CVE-2023-27524	0.972950000	0.998560000	Link
CVE-2023-27372	0.973490000	0.998880000	Link
CVE-2023-27350	0.972040000	0.998120000	Link
CVE-2023-26469	0.938630000	0.990950000	Link
CVE-2023-26360	0.963530000	0.995320000	Link
CVE-2023-26035	0.969280000	0.997050000	Link
CVE-2023-25717	0.957880000	0.994060000	Link
CVE-2023-25194	0.969270000	0.997050000	Link
CVE-2023-2479	0.963600000	0.995350000	Link
CVE-2023-24489	0.973920000	0.999100000	Link
CVE-2023-23752	0.952140000	0.993020000	Link
CVE-2023-23397	0.923530000	0.989240000	Link
CVE-2023-23333	0.963260000	0.995240000	Link
CVE-2023-22527	0.965680000	0.996030000	Link
CVE-2023-22518	0.964830000	0.995680000	Link
CVE-2023-22515	0.972680000	0.998400000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-21839	0.958450000	0.994140000	Link
CVE-2023-21554	0.959700000	0.994390000	Link
CVE-2023-20887	0.962160000	0.994970000	Link
CVE-2023-1671	0.967910000	0.996670000	Link
CVE-2023-0669	0.969030000	0.996970000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 12 Apr 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Schwachstelle in unbound

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um eine laufende Instanz zu manipulieren, Informationen offenzulegen oder einen Denial-of-Service auszulösen.

- Link

—

Fri, 12 Apr 2024

[UPDATE] [hoch] Microsoft SQL Server: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft SQL Server 2019, Microsoft SQL Server 2022 und Microsoft SQL Server (MSSQL) ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 12 Apr 2024

[NEU] [UNGEPATCHT] [hoch] ffmpeg: Schwachstelle ermöglicht Codeausführung und DoS

Ein lokaler Angreifer kann eine Schwachstelle in ffmpeg ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Thu, 11 Apr 2024

[NEU] [hoch] Juniper Produkte: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Juniper Produkten ausnutzen

um Denial of Service Zustände zu verursachen, Informationen offenzulegen und Sicherheitsmechanismen zu umgehen.
- Link

—

Thu, 11 Apr 2024

[NEU] [hoch] VMware Tanzu Spring Framework: Schwachstelle ermöglicht Manipulation von Daten

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in VMware Tanzu Spring Framework ausnutzen, um Daten zu manipulieren oder Informationen offenzulegen.
- Link

—

Thu, 11 Apr 2024

[NEU] [hoch] GitLab: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Thu, 11 Apr 2024

[NEU] [hoch] Google Chrome: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen und weitere, nicht spezifizierte Auswirkungen zu verursachen.
- Link

—

Thu, 11 Apr 2024

[UPDATE] [hoch] cURL: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in cURL ausnutzen, um Dateien zu manipulieren, Daten offenzulegen oder einen Denial of Service zu verursachen.
- Link

—

Thu, 11 Apr 2024

[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht Denial of Service und Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in QEMU ausnutzen, um einen Denial of Service herbeizuführen und potenziell um beliebigen Programmcode auszuführen.
- Link

—

Thu, 11 Apr 2024

[UPDATE] [hoch] Squid: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Squid ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.

- Link

—

Thu, 11 Apr 2024

[UPDATE] [hoch] Squid: Mehrere Schwachstellen ermöglichen Denial of Service

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

- Link

—

Thu, 11 Apr 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

—

Thu, 11 Apr 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

—

Thu, 11 Apr 2024

[UPDATE] [hoch] util-linux: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein lokaler Angreifer kann eine Schwachstelle in util-linux ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 10 Apr 2024

[NEU] [hoch] Paessler PRTG: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Paessler PRTG ausnutzen, um beliebigen Programmcode auszuführen einen Cross Site Scripting Angriff durchzuführen oder Informationen offenzulegen.

- Link

—

Wed, 10 Apr 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programm-

code auszuführen.
- Link

—

Wed, 10 Apr 2024

[NEU] [hoch] Microsoft Office: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft 365 Apps, Microsoft Office, Microsoft SharePoint, Microsoft SharePoint Server 2016 und Microsoft SharePoint Server 2019 ausnutzen, um beliebigen Programmcode auszuführen oder Cross-Site Scripting (XSS)-Angriffe durchzuführen.
- Link

—

Wed, 10 Apr 2024

[NEU] [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

—

Wed, 10 Apr 2024

[UPDATE] [hoch] IBM DB2: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in IBM DB2 ausnutzen, um einen Denial of Service Angriff durchzuführen, Informationen offenzulegen oder beliebigen Programmcode auszuführen.
- Link

—

Wed, 10 Apr 2024

[NEU] [hoch] Microsoft Defender: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Microsoft Defender ausnutzen, um seine Privilegien zu erhöhen oder beliebigen Programmcode auszuführen.
- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
4/14/2024	[Fedora 38 : kernel (2024-a56a47ef1b)]	critical
4/13/2024	[Fedora 39 : kernel (2024-33a9ea72d1)]	critical
4/13/2024	[Siemens Scalance W1750D Buffer Copy without Checking Size of Input (CVE-2023-45615)]	critical
4/13/2024	[Siemens Scalance W1750D Buffer Copy without Checking Size of Input (CVE-2023-45616)]	critical
4/13/2024	[Siemens Scalance W1750D Buffer Copy without Checking Size of Input (CVE-2023-35982)]	critical
4/13/2024	[Siemens Scalance W1750D Buffer Copy without Checking Size of Input (CVE-2023-35980)]	critical
4/13/2024	[Siemens Scalance W1750D Buffer Copy without Checking Size of Input (CVE-2023-45614)]	critical
4/13/2024	[Siemens Scalance W1750D Buffer Copy without Checking Size of Input (CVE-2023-35981)]	critical
4/15/2024	[Fedora 39 : chromium (2024-fe9a675a37)]	high
4/14/2024	[Fedora 38 : chromium (2024-f94660c56d)]	high
4/14/2024	[Fedora 39 : libopenmpt (2024-90b3798199)]	high
4/14/2024	[Fedora 38 : libopenmpt (2024-85b6c6fa92)]	high
4/14/2024	[Slackware Linux 15.0 / current less Vulnerability (SSA:2024-105-01)]	high
4/14/2024	[Debian dsa-5659 : trafficserver - security update]	high
4/13/2024	[Fedora 38 : rust-h2 (2024-c5b42e6462)]	high
4/13/2024	[Fedora 39 : rust-h2 (2024-638f25a317)]	high
4/13/2024	[Debian dsa-5657 : xdmx - security update]	high
4/13/2024	[Wireshark 4.0.x < 4.0.14 A Vulnerability (macOS)]	high
4/13/2024	[Wireshark 4.0.x < 4.0.14 A Vulnerability]	high
4/13/2024	[Oracle Linux 8 : httpd:2.4/mod_http2 (ELSA-2024-1786)]	high

Datum	Schwachstelle	Bewertung
4/13/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : xorg-x11-server (SUSE-SU-2024:1262-1)]	high
4/13/2024	[SUSE SLES12 Security Update : kernel (Live Patch 54 for SLE 12 SP5) (SUSE-SU-2024:1275-1)]	high
4/13/2024	[SUSE SLES15 Security Update : xorg-x11-server (SUSE-SU-2024:1260-1)]	high
4/13/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : xwayland (SUSE-SU-2024:1264-1)]	high
4/13/2024	[SUSE SLES15 Security Update : kernel RT (Live Patch 10 for SLE 15 SP5) (SUSE-SU-2024:1273-1)]	high
4/13/2024	[SUSE SLES15 Security Update : kernel (Live Patch 6 for SLE 15 SP5) (SUSE-SU-2024:1274-1)]	high
4/13/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : webkit2gtk3 (SUSE-SU-2024:1270-1)]	high
4/13/2024	[SUSE SLES12 Security Update : xorg-x11-server (SUSE-SU-2024:1263-1)]	high
4/13/2024	[SUSE SLED15 / SLES15 Security Update : xorg-x11-server (SUSE-SU-2024:1261-1)]	high
4/13/2024	[SUSE SLES15 Security Update : kernel (Live Patch 40 for SLE 15 SP2) (SUSE-SU-2024:1257-1)]	high
4/13/2024	[SUSE SLES15 Security Update : webkit2gtk3 (SUSE-SU-2024:1269-1)]	high
4/13/2024	[SUSE SLES15 Security Update : kernel (Live Patch 1 for SLE 15 SP5) (SUSE-SU-2024:1252-1)]	high
4/13/2024	[SUSE SLES15 Security Update : kernel (Live Patch 10 for SLE 15 SP5) (SUSE-SU-2024:1278-1)]	high
4/13/2024	[SUSE SLES15 Security Update : kernel (Live Patch 42 for SLE 15 SP3) (SUSE-SU-2024:1276-1)]	high
4/13/2024	[Debian dsa-5658 : affs-modules-6.1.0-11-4kc-malta-di - security update]	high

Datum	Schwachstelle	Bewertung
4/13/2024	[FreeBSD : chromium – multiple security fixes (7314942b-0889-46f0-b02b-2c60aabe4a82)]	high
4/13/2024	[Siemens Scalance W1750D Improper Input Validation (CVE-2023-45621)]	high
4/13/2024	[Siemens Scalance W1750D Improper Input Validation (CVE-2023-45623)]	high
4/13/2024	[Siemens Scalance W1750D Improper Input Validation (CVE-2023-45618)]	high
4/13/2024	[Siemens Scalance W1750D Improper Input Validation (CVE-2023-45620)]	high
4/13/2024	[Siemens Scalance W1750D Improper Input Validation (CVE-2023-45619)]	high
4/13/2024	[Siemens Scalance W1750D Improper Input Validation (CVE-2023-45622)]	high
4/13/2024	[Siemens Scalance W1750D Improper Neutralization of Special Elements used in a Command (CVE-2023-45625)]	high
4/13/2024	[Siemens Scalance W1750D Improper Input Validation (CVE-2023-45624)]	high
4/13/2024	[Siemens Scalance W1750D Improper Input Validation (CVE-2023-45626)]	high
4/13/2024	[Siemens Scalance W1750D Improper Input Validation (CVE-2023-45617)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Fri, 12 Apr 2024

Terratec dmx_6fire USB 1.23.0.02 Unquoted Service Path

Terratec dmx_6fire USB version 1.23.0.02 suffers from an unquoted service path vulnerability.

- Link

—

” “Fri, 12 Apr 2024

Ray OS 2.6.3 Command Injection

The Ray Project dashboard contains a CPU profiling page, and the format parameter is not validated before being inserted into a system command executed in a shell, allowing for arbitrary command execution. If the system is configured to allow passwordless sudo (a setup some Ray configurations require) this will result in a root shell being returned to the user. If not configured, a user level shell will be returned. Versions 2.6.3 and below are affected.

- Link

—

” “Fri, 12 Apr 2024

WordPress Playlist For Youtube 1.32 Cross Site Scripting

WordPress Playlist for Youtube plugin version 1.32 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Fri, 12 Apr 2024

MinIO Privilege Escalation

MinIO versions prior to 2024-01-31T20-20-33Z suffer from a privilege escalation vulnerability.

- Link

—

” “Thu, 11 Apr 2024

Trimble TM4Web 22.2.0 Privilege Escalation / Access Code Disclosure

An access control issue in Trimble TM4Web version 22.2.0 allows unauthenticated attackers to access a specific crafted URL path to retrieve the last registration access code and use this access code to register a valid account. If the access code was used to create an Administrator account, attackers are also able to register new Administrator accounts with full rights and privileges.

- Link

—

” “Thu, 11 Apr 2024

Concrete CMS 9.2.7 Cross Site Scripting / Open Redirect

Concrete CMS version 9.2.7 suffers from information disclosure, open redirection, and persistent cross site scripting vulnerabilities.

- Link

—

” “Thu, 11 Apr 2024

GUnet OpenEclass E-learning 3.15 File Upload / Command Execution

GUnet OpenEclass E-learning platform version 3.15 suffers from an unrestricted file upload vulnerabi-

lity in certbadge.php that allows for remote command execution.

- Link

—

” “Thu, 11 Apr 2024

Windows Kernel Subkey List Use-After-Free

The Windows Kernel suffers from a subkey list use-after-free vulnerability due to a mishandling of partial success in CmpAddSubKeyEx.

- Link

—

” “Wed, 10 Apr 2024

CHAOS RAT 5.0.1 Remote Command Execution

CHAOS RAT web panel version 5.0.1 is vulnerable to command injection, which can be triggered from a cross site scripting attack, allowing an attacker to takeover the RAT server.

- Link

—

” “Wed, 10 Apr 2024

Joomla SP Page Builder 5.2.7 SQL Injection

Joomla SP Page Builder component version 5.2.7 suffers from a remote SQL injection vulnerability.

- Link

—

” “Tue, 09 Apr 2024

Flightio.com SQL Injection

Flightio.com suffers from a remote SQL injection vulnerability. The researchers reporting this claimed the site has not responded to their reports so we are posting this to add visibility to the issue.

- Link

—

” “Mon, 08 Apr 2024

WordPress Travelscape Theme 1.0.3 Arbitrary File Upload

WordPress Travelscape theme version 1.0.3 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Mon, 08 Apr 2024

Daily Expense Manager 1.0 SQL Injection

Daily Expense Manager version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 08 Apr 2024

Open Source Medicine Ordering System 1.0 SQL Injection

Open Source Medicine Ordering System version 1.0 suffers from a remote SQL Injection vulnerability.
- Link

—

” “Mon, 08 Apr 2024

ZenML Remote Privilege Escalation

ZenML allows for remote privilege escalation because the /api/v1/users/{user_name_or_id}/activate REST API endpoint allows access on the basis of a valid username along with a new password in the request body. This is the proof of concept exploit. All ZenML versions below 0.46.7 are vulnerable, with the exception being patched versions 0.44.4, 0.43.1, and 0.42.2.
- Link

—

” “Mon, 08 Apr 2024

Invision Community 4.7.16 Remote Code Execution

Invision Community versions 4.7.16 and below suffer from a remote code execution vulnerability in toolbar.php.
- Link

—

” “Mon, 08 Apr 2024

Invision Community 4.7.15 SQL Injection

Invision Community versions 4.4.0 through 4.7.15 suffer from a remote SQL injection vulnerability in store.php.
- Link

—

” “Mon, 08 Apr 2024

Open eShop 2.7.0 Cross Site Scripting

Open eShop version 2.7.0 suffers from a cross site scripting vulnerability.
- Link

—

” “Mon, 08 Apr 2024

HTMLy 2.9.6 Cross Site Scripting

HTMLy version 2.9.6 suffers from a persistent cross site scripting vulnerability.
- Link

—

” “Mon, 08 Apr 2024

UP-RESULT 0.1 2024 SQL Injection

UP-RESULT version 0.1 2024 suffers from a remote SQL injection vulnerability.
- Link

—

” “Mon, 08 Apr 2024

Trojan.Win32.Razy.abc MVID-2024-0678 Insecure Permissions

Trojan.Win32.Razy.abc malware suffers from an insecure permissions vulnerability.

- Link

—

” “Mon, 08 Apr 2024

AnyDesk 7.0.15 Unquoted Service Path

AnyDesk version 7.0.15 suffers from an unquoted service path vulnerability.

- Link

—

” “Mon, 08 Apr 2024

PowerVR DevmemIntUnexportCtx Use-After-Free

PowerVR has an issue where DevmemIntUnexportCtx destroys export before unlinking it, leading to a use-after-free condition.

- Link

—

” “Fri, 05 Apr 2024

Visual Planning 8 Arbitrary File Read

Authenticated attackers can exploit a weakness in the XML parser functionality of the Visual Planning application in order to obtain read access to arbitrary files on the application server. Depending on configured access permissions, this vulnerability could be used by an attacker to exfiltrate secrets stored on the local file system. All versions prior to Visual Planning 8 (Build 240207) are affected.

- Link

—

” “Fri, 05 Apr 2024

Visual Planning 8 Authentication Bypass

Unauthenticated attackers can exploit a weakness in the password reset functionality of the Visual Planning application in order to obtain access to arbitrary user accounts including administrators. In case administrative (in the context of Visual Planning) accounts are compromised, attackers can install malicious modules into the application to take over the application server hosting the Visual Planning application. All versions prior to Visual Planning 8 (Build 240207) are affected.

- Link

—

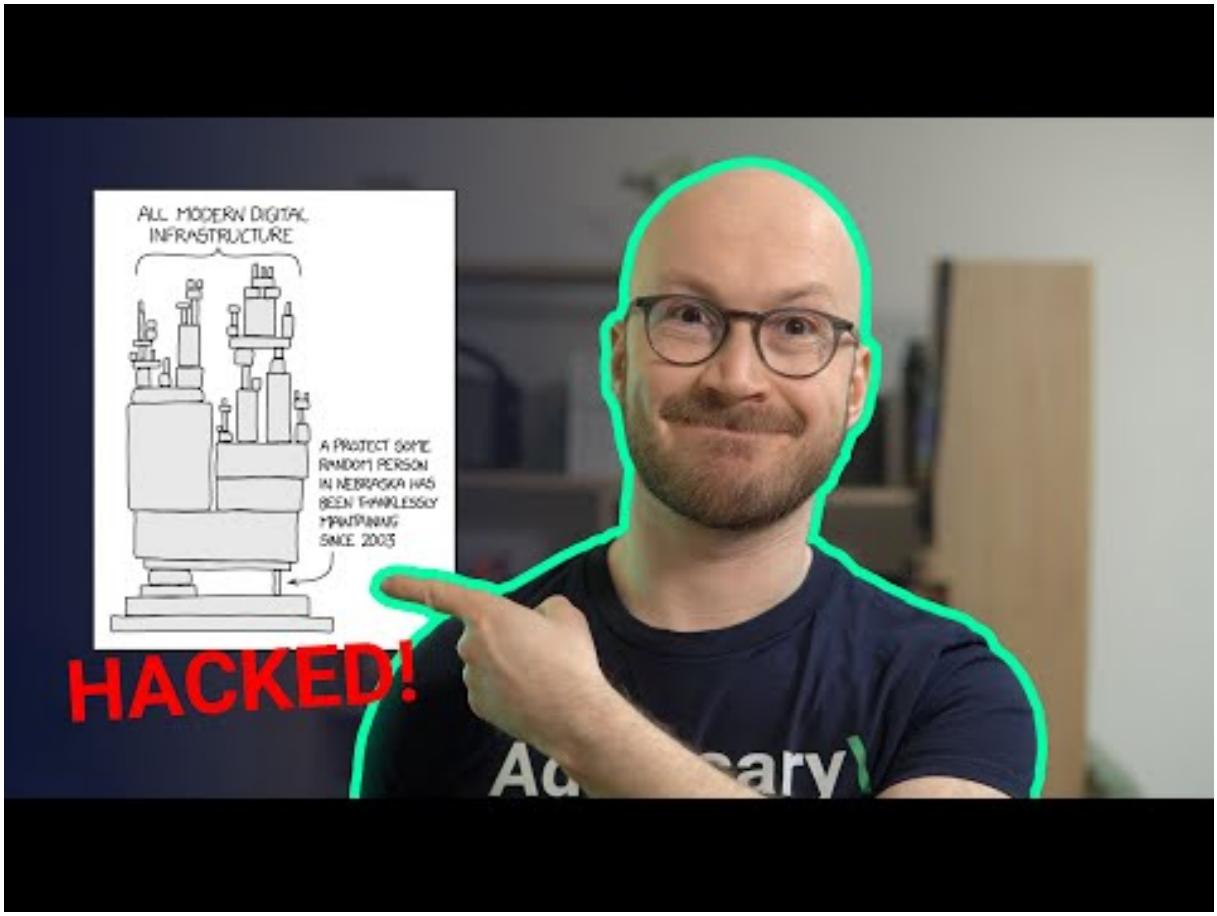
”

4.2 0-Days der letzten 5 Tage

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Oh wow, this was *very* close: xz-utils was backdoored



Zum Youtube Video

6 Cyberangriffe: (Apr)

Datum	Opfer	Land	Information
2024-04-11	Taiwan United Renewable Energy Corporation (URECO)	[TWN]	Link
2024-04-11	Swinomish Casino and Lodge	[USA]	Link
2024-04-11	Iddink Learning Materials	[NLD]	Link
2024-04-10	Ville de Saint-Nazaire et son agglomération	[FRA]	Link
2024-04-09	The Heritage Foundation	[USA]	Link
2024-04-07	CVS Group	[GBR]	Link
2024-04-07	St. Elisabeth-Stiftung	[DEU]	Link
2024-04-07	GBI-Genios Deutsche Wirtschaftsdatenbank GmbH	[DEU]	Link
2024-04-05	Targus	[USA]	Link
2024-04-04	Communauté de communes du bassin mussipontain	[FRA]	Link
2024-04-04	Bielefeld Fertility Center	[DEU]	Link
2024-04-03	New Mexico Highlands University	[USA]	Link
2024-04-02	Comté de Jackson	[USA]	Link
2024-04-02	Prepay Technologies	[ESP]	Link
2024-04-02	Riley County	[USA]	Link
2024-04-02	NorthBay Health	[USA]	Link

7 Ransomware-Erpressungen: (Apr)

Datum	Opfer	Ransomware-Grupppe	Webseite

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.