Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240411

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

Befehlsschmuggel: Kritische Lücke in Programmiersprachen unter Windows

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

- 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

—

HP Poly CCX IP-Telefone erlauben unbefugten Zugriff

Die Poly CCX IP Phones von HP erlauben aufgrund fehlender Kontrollen unbefugten Zugriff. Aktualisierte Firmware schafft Abhilfe.

- Link

—

SAP-Patchday: Zehn Sicherheitsmitteilungen im April

Insgesamt zehn Sicherheitsnotizen gibt SAP am April-Patchday heraus. Drei der behandelten Lücken gelten als hochriskant.

- Link

—

Nvidias Chatbot-App ChatRTX ist für Schadcode-Attacken anfällig

In einer aktualisierten Ausgabe haben die Entwickler von Nvidia ChatRTX gegen mögliche Attacken abgesichert.

- Link

—

Dell-Server: BIOS-Lücke als Einfallstor für Angreifer

Ein wichtiges Sicherheitsupdate schließt eine Schwachstelle im BIOS von Servern des Computerherstellers Dell.

- Link

—

Lexmark: Hochriskante Lücken erlauben Codeschmuggel auf Drucker

Lexmark warnt vor Sicherheitslücken in diversen Drucker-Firmwares. Angreifer können Schadcode einschleusen. Updates sind verfügbar.

- Link

—

Sicherheitslücken: DoS-Attacken auf IBM-Datenbank Db2 möglich

Angreifer können an mehreren Lücken in IBM App Connect Enterprise, Db2 und Rational Build Forge ansetzen.

- 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	0.987470000	Link
CVE-2023-6553	0.916210000	0.988510000	Link
CVE-2023-5360	0.967230000	0.996410000	Link
CVE-2023-4966	0.964860000	0.995700000	Link
CVE-2023-47246	0.940270000	0.991140000	Link
CVE-2023-46805	0.964290000	0.995560000	Link
CVE-2023-46747	0.971350000	0.997840000	Link
CVE-2023-46604	0.973060000	0.998600000	Link
CVE-2023-43177	0.927670000	0.989810000	Link
CVE-2023-42793	0.970710000	0.997550000	Link
CVE-2023-39143	0.942940000	0.991490000	Link
CVE-2023-38646	0.928720000	0.989880000	Link
CVE-2023-38203	0.967010000	0.996360000	Link
CVE-2023-38035	0.973610000	0.998930000	Link
CVE-2023-36845	0.966640000	0.996240000	Link
CVE-2023-35813	0.905250000	0.987680000	Link
CVE-2023-3519	0.911860000	0.988210000	Link
CVE-2023-35082	0.950590000	0.992770000	Link
CVE-2023-35078	0.962310000	0.994970000	Link
CVE-2023-34993	0.944980000	0.991930000	Link
CVE-2023-34960	0.935410000	0.990600000	Link
CVE-2023-34634	0.925600000	0.989540000	Link
CVE-2023-34362	0.960290000	0.994510000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34039	0.907130000	0.987850000	Link
CVE-2023-3368	0.918440000	0.988750000	Link
CVE-2023-33246	0.973150000	0.998670000	Link
CVE-2023-32315	0.973840000	0.999060000	Link
CVE-2023-32235	0.911650000	0.988170000	Link
CVE-2023-30625	0.948330000	0.992450000	Link
CVE-2023-30013	0.956380000	0.993790000	Link
CVE-2023-29300	0.963460000	0.995290000	Link
CVE-2023-29298	0.926460000	0.989640000	Link
CVE-2023-28771	0.921620000	0.989040000	Link
CVE-2023-28432	0.943220000	0.991560000	Link
CVE-2023-28121	0.943690000	0.991630000	Link
CVE-2023-27524	0.972950000	0.998550000	Link
CVE-2023-27372	0.973490000	0.998880000	Link
CVE-2023-27350	0.972040000	0.998100000	Link
CVE-2023-26469	0.938630000	0.990950000	Link
CVE-2023-26360	0.963570000	0.995320000	Link
CVE-2023-26035	0.969280000	0.997040000	Link
CVE-2023-25717	0.957880000	0.994030000	Link
CVE-2023-25194	0.969270000	0.997040000	Link
CVE-2023-2479	0.963600000	0.995330000	Link
CVE-2023-24489	0.973810000	0.999040000	Link
CVE-2023-23752	0.952140000	0.993000000	Link
CVE-2023-23397	0.923530000	0.989240000	Link
CVE-2023-23333	0.963260000	0.995220000	Link
CVE-2023-22527	0.965680000	0.996020000	Link
CVE-2023-22518	0.969490000	0.997110000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-22515	0.972680000	0.998370000	Link
CVE-2023-21839	0.958450000	0.994110000	Link
CVE-2023-21554	0.959700000	0.994350000	Link
CVE-2023-20887	0.964080000	0.995480000	Link
CVE-2023-1671	0.967910000	0.996650000	Link
CVE-2023-0669	0.969030000	0.996960000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

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

[NEU] [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

—

Wed, 10 Apr 2024

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

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

—

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

—

Wed, 10 Apr 2024

[NEU] [hoch] Microsoft Developer Tools: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Microsoft .NET Framework, Microsoft Visual Studio 2019 und Microsoft Visual Studio 2022 ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 10 Apr 2024

[NEU] [hoch] Microsoft Azure: Mehrere Schwachstellen

Ein Angreifer kann diese Schwachstellen in Azure ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder seine Rechte zu erweitern.

- Link

—

Wed, 10 Apr 2024

[NEU] [hoch] TIBCO JasperReports: Mehrere Schwachstellen

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in TIBCO JasperReports ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder Cross-Site Scripting (XSS)-Angriffe durchzuführen.

- Link

—

Wed, 10 Apr 2024

[NEU] [hoch] Fortinet FortiSandbox: Mehrere Schwachstellen

Ein lokaler oder entfernter authentifizierter Angreifer kann mehrere Schwachstellen in Fortinet FortiSandbox ausnutzen, um beliebigen Code auszuführen, Dateien zu manipulieren oder vertrauliche Informationen offenzulegen.

- Link

—

Wed, 10 Apr 2024

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um einen Denial of Service Angriff durchzuführen und um Sicherheitsmechanismen zu umgehen.

- Link

—

Wed, 10 Apr 2024

[NEU] [hoch] QEMU: Schwachstelle ermöglicht Codeausführung und DoS

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

- Link

—

Wed, 10 Apr 2024

[NEU] [hoch] Fortinet FortiOS: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Fortinet FortiOS und Fortinet FortiProxy ausnutzen, um Informationen offenzulegen.

- Link

—

Wed, 10 Apr 2024

[UPDATE] [hoch] Linux Kernel (ksmbd): Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of Service-Zustand herbeizuführen, Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen, Privilegien zu erweitern und beliebigen Code auszuführen.

- Link

—

Wed, 10 Apr 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

—

Wed, 10 Apr 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

—

Wed, 10 Apr 2024

[UPDATE] [hoch] EDK2 NetworkPkg IP stack implementation: Mehrere Schwachstellen

Ein Angreifer aus dem angrenzenden Netzwerk oder ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der EDK2 NetworkPkg IP stack implementation ausnutzen, um beliebigen Programmcode auszuführen, vertrauliche Informationen offenzulegen und einen Denial of Service Zustand auszulösen.

- Link

—

Wed, 10 Apr 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien

zu erhöhen.
- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
4/10/2024	[Fedora 39 : rpm-ostree (2024-4afd3d38ae)]	critical
4/10/2024	[Palo Alto Networks PAN-OS 9.0.x < 9.0.17-h2 / 9.1.x < 9.1.17 / 10.0.x < 10.0.13 / 10.1.x < 10.1.10 / 10.2.x < 10.2.5 / 11.0.x < 11.0.2 Vulnerability]	critical
4/10/2024	[Google Chrome < 123.0.6312.122 Multiple Vulnerabilities]	critical
4/10/2024	[Google Chrome < 123.0.6312.122 Multiple Vulnerabilities]	critical
4/10/2024	[RHEL 8 / 9 : GitOps 1.12.1- Argo CD CLI and MicroShift GitOps (RHSA-2024:1752)]	critical
4/9/2024	[Oracle Linux 8 : Unbreakable Enterprise kernel-container (ELSA-2024-12275)]	high
4/9/2024	[Oracle Linux 7 : Unbreakable Enterprise kernel-container (ELSA-2024-12274)]	high
4/9/2024	[Oracle Linux 7 / 8 : Unbreakable Enterprise kernel (ELSA-2024-12271)]	high
4/11/2024	[Oracle Linux 9 : unbound (ELSA-2024-1750)]	high
4/10/2024	[Fedora 38 : emacs (2024-53b69fdd40)]	high
4/10/2024	[Fedora 38 : dotnet8.0 (2024-1ef4b14811)]	high
4/10/2024	[Fedora 39 : dotnet8.0 (2024-6462d0aa27)]	high
4/10/2024	[Debian dla-3785 : gtkwave - security update]	high
4/10/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : util-linux (SUSE-SU-2024:1172-1)]	high

Datum	Schwachstelle	Bewertung
4/10/2024	[SUSE SLES15 Security Update : util-linux (SUSE-SU-2024:1170-1)]	high
4/10/2024	[SUSE SLES15 Security Update : kernel RT (Live Patch 0 for SLE 15 SP5) (SUSE-SU-2024:1181-1)]	high
4/10/2024	[SUSE SLED12 / SLES12 Security Update : util-linux (SUSE-SU-2024:1171-1)]	high
4/10/2024	[SUSE SLES15 Security Update : util-linux (SUSE-SU-2024:1169-1)]	high
4/10/2024	[Fedora 39 : dotnet7.0 (2024-8420247612)]	high
4/10/2024	[Security Update for Microsoft .NET Core (April 2024)]	high
4/10/2024	[Security Updates for Azure CycleCloud (April 2024)]	high
4/10/2024	[Palo Alto Networks PAN-OS 10.1.x < 10.1.11 / 10.2.x < 10.2.5 / 11.0.x < 11.0.3 Vulnerability]	high
4/10/2024	[RHEL 9 : unbound (RHSA-2024:1750)]	high
4/10/2024	[RHEL 7 : kernel (RHSA-2024:1746)]	high
4/10/2024	[RHEL 7 : kernel (RHSA-2024:1747)]	high
4/10/2024	[Palo Alto Networks PAN-OS 10.1.x < 10.1.12 / 10.2.x < 10.2.8 / 11.0.x < 11.0.4 Vulnerability]	high
4/10/2024	[Palo Alto Networks PAN-OS 10.2.x < 10.2.7-h3 / 11.0.x < 11.0.4 / 11.1.x < 11.1.2 Vulnerability]	high
4/10/2024	[Palo Alto Networks PAN-OS 8.1.x < 8.1.24 / 9.0.x < 9.0.17 / 9.1.x < 9.1.15-h1 / 10.0.x < 10.0.12 Vulnerability]	high
4/10/2024	[Palo Alto Networks PAN-OS 9.0.x < 9.0.17-h4 / 9.1.x < 9.1.17 / 10.1.x < 10.1.12 / 10.2.x < 10.2.8 / 11.0.x < 11.0.3 Vulnerability]	high
4/10/2024	[AlmaLinux 9 : less (ALSA-2024:1692)]	high
4/10/2024	[AlmaLinux 9 : varnish (ALSA-2024:1691)]	high
4/10/2024	[AlmaLinux 9 : nodejs:20 (ALSA-2024:1688)]	high
4/10/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : util-linux vulnerability (USN-6719-2)]	high

Datum	Schwachstelle	Bewertung
4/10/2024	[Security Updates for Microsoft SQL Server ODBC Driver (April 2024)]	high
4/10/2024	[Security Updates for Microsoft SQL Server OLE DB Driver (April 2024)]	high
4/10/2024	[Security Update for Microsoft .NET Core SDK (April 2024)]	high
4/10/2024	[AlmaLinux 8 : varnish (ALSA-2024:1690)]	high
4/10/2024	[Oracle Linux 8 : virt:kvm_utils3 (ELSA-2024-12276)]	high
4/10/2024	[AlmaLinux 8 : nodejs:20 (ALSA-2024:1687)]	high
4/10/2024	[Ubuntu 20.04 LTS / 22.04 LTS : Squid vulnerabilities (USN-6728-1)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“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

—

” “Fri, 05 Apr 2024

Visual Planning REST API 2.0 Authentication Bypass

A wildcard injection inside a prepared SQL statement was found in an undocumented Visual Planning 8 REST API route. The combination of fuzzy matching (via LIKE operator) and user-controlled input allows exfiltrating the REST API key based on distinguishable server responses. If exploited, attackers are able to gain administrative access to the REST API version 2.0.

- Link

—

” “Fri, 05 Apr 2024

Feng Office 3.10.8.21 Cross Site Scripting

Feng Office version 3.10.8.21 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 print/render/racer.inc SQL Injection

DerbyNet 9.0 suffers from a remote SQL injection vulnerability in print/render/racer.inc.

- Link

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 print/render/award.inc SQL Injection

DerbyNet 9.0 suffers from a remote SQL injection vulnerability in print/render/award.inc.

- Link

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 ajax/query.slide.next.inc SQL Injection

DerbyNet 9.0 suffers from a remote SQL injection vulnerability in ajax/query.slide.next.inc.

- Link

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 playlist.php Cross Site Scripting

DerbyNet version 9.0 suffers from a cross site scripting vulnerability in playlist.php.

- Link

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 racer-results.php Cross Site Scripting

DerbyNet version 9.0 suffers from a cross site scripting vulnerability in racer-results.php.

- Link

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 inc/kisosks.inc Cross Site Scripting

DerbyNet version 9.0 suffers from a cross site scripting vulnerability in inc/kiosks.inc.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Tue, 09 Apr 2024

ZDI-24-364: Arista NG Firewall ReportEntry SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Tue, 09 Apr 2024

ZDI-24-363: Microsoft Windows Installer Service Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 09 Apr 2024

ZDI-24-362: Microsoft Azure Private 5G Core InitialUEMessage Improper Input Validation Denial-of-Service Vulnerability

- Link

—

” “Tue, 09 Apr 2024

ZDI-24-361: Microsoft Windows Internet Shortcut SmartScreen Bypass Vulnerability

- Link

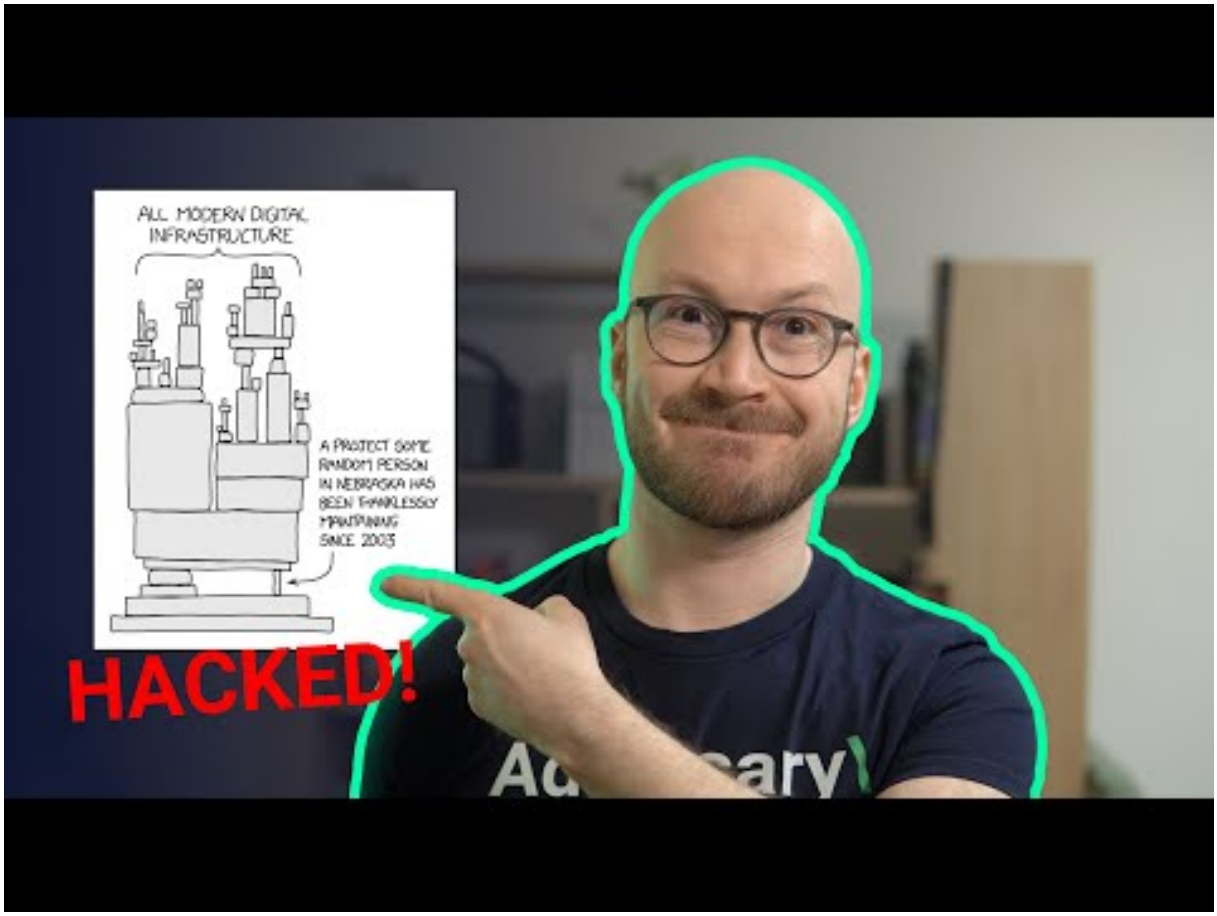
—

”

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
2024-04-10	Ville de Saint-Nazaire et son agglomération	[FRA]	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
2024-04-03	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

7 Ransomware-Erpressungen: (Apr)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-10	[F???s???? & ??????t]	play	Link
2024-04-10	[Inszone Insurance Services]	hunters	Link
2024-04-10	[Nexperia]	dunghill	Link
2024-04-10	[Samart]	akira	Link
2024-04-10	[Robertson Cheatham Farmers]	hunters	Link
2024-04-10	[specialoilfield.com]	lockbit3	Link
2024-04-09	[Consilux (Brazil)]	akira	Link
2024-04-09	[processsolutions.com]	blackbasta	Link
2024-04-09	[numotion.com]	blackbasta	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-09	[siemensmfg.com]	blackbasta	Link
2024-04-09	[Parklane Group]	blackbasta	Link
2024-04-09	[sermo.com]	blackbasta	Link
2024-04-09	[schlesingerlaw.com]	blackbasta	Link
2024-04-09	[robar.com]	blackbasta	Link
2024-04-09	[atlascontainer.com]	blackbasta	Link
2024-04-09	[patersoncooke.com]	blackbasta	Link
2024-04-09	[arch-con.com]	blackbasta	Link
2024-04-09	[New Production Concept]	dragonforce	Link
2024-04-09	[Precision Pulley & Idler]	blacksuit	Link
2024-04-09	[columbiapipe.com]	blackbasta	Link
2024-04-09	[T A Khoury]	hunters	Link
2024-04-09	[Kadushisoft]	dragonforce	Link
2024-04-09	[Saint Cecilia’s Church of England School]	dragonforce	Link
2024-04-09	[Swansea & South Wales]	dragonforce	Link
2024-04-09	[MajuHome Concept]	dragonforce	Link
2024-04-09	[Team Locum]	dragonforce	Link
2024-04-09	[Rigcon]	dragonforce	Link
2024-04-09	[Vstblekinge Miljo]	dragonforce	Link
2024-04-09	[JM Heaford]	blacksuit	Link
2024-04-09	[Eagle Hydraulic Components]	blacksuit	Link
2024-04-09	[MULTI-FILL]	blacksuit	Link
2024-04-09	[Central Carolina Insurance Agency Inc.]	bianlian	Link
2024-04-09	[Panacea Healthcare Services]	bianlian	Link
2024-04-09	[Baca County Feedyard, Inc]	ransomhub	Link
2024-04-09	[Brewer & Company of WV]	blacksuit	Link
2024-04-09	[Olea Kiosks]	blacksuit	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-09	[Hudson Supplies]	blacksuit	Link
2024-04-09	[Homeocan]	blacksuit	Link
2024-04-09	[Macuz]	ciphbit	Link
2024-04-09	[speditionlangen.de]	mallox	Link
2024-04-09	[maccarinelli.it]	qilin	Link
2024-04-08	[Skyway Coach Lines and Shuttle Services – skywaycoach.ca]	ransomhub	Link
2024-04-08	[John R. Wood Properties]	medusa	Link
2024-04-08	[Paulmann Licht]	hunters	Link
2024-04-08	[PGF Technology Group]	akira	Link
2024-04-08	[REV Drill Sales & Rentals]	akira	Link
2024-04-08	[PHARMACY ETTORE FLORIO SNC - Online Pharmacy Italy]	ransomhub	Link
2024-04-05	[Paducah Dermatology]	medusa	Link
2024-04-05	[Domestic Violence Project, Inc]	medusa	Link
2024-04-05	[Rairdon Automotive Group]	medusa	Link
2024-04-05	[Integration International]	medusa	Link
2024-04-06	[Tarrant Appraisal District]	medusa	Link
2024-04-08	[Speditionweise.de]	cloak	Link
2024-04-08	[Mahoney Foundry, Inc.]	8base	Link
2024-04-08	[DUNN, PITTMAN, SKINNER and CUSHMAN, PLLC]	8base	Link
2024-04-08	[Inno-soft Info Systems Pte Ltd]	8base	Link
2024-04-08	[Z Development Services, LLC]	8base	Link
2024-04-08	[Change HealthCare - OPTUM Group - United HealthCare Group]	ransomhub	Link
2024-04-07	[PalauGov]	dragonforce	Link
2024-04-07	[Ellsworth Cooperative Creamery]	blacksuit	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-07	[SERVICES INFORMATIQUES POUR PROFESSIONNELS(SIP)]	blacksuit	Link
2024-04-07	[Malaysian Industrial Development Finance]	rhysida	Link
2024-04-07	[easchangesystems]	qilin	Link
2024-04-06	[Carrozzeria Aretusa srl]	ransomhub	Link
2024-04-06	[HCI Systems, Inc.]	ransomhub	Link
2024-04-06	[Madero]	qilin	Link
2024-04-06	[Chambers Construction]	bianlian	Link
2024-04-06	[On Q Financial, LLC]	bianlian	Link
2024-04-06	[Better Accounting Solutions]	ransomhub	Link
2024-04-06	[TermoPlastic S.R.L]	ciphbit	Link
2024-04-05	[truehomes.com]	lockbit3	Link
2024-04-04	[Good Morning]	donutleaks	Link
2024-04-05	[casio india]	stormous	Link
2024-04-05	[emalon.co.il]	malekteam	Link
2024-04-05	[Aussizz Group]	dragonforce	Link
2024-04-05	[Doctorim]	malekteam	Link
2024-04-05	[Agencia Host]	ransomhub	Link
2024-04-05	[Commerce Dental Group]	ciphbit	Link
2024-04-04	[Sit]	play	Link
2024-04-04	[Guy’s Floor Service]	play	Link
2024-04-04	[Everbrite]	play	Link
2024-04-03	[Orientrose Contracts]	medusa	Link
2024-04-03	[Sutton Dental Arts]	medusa	Link
2024-04-04	[Inspection Services]	akira	Link
2024-04-04	[Radiant Canada]	akira	Link
2024-04-04	[Constelacion Savings and Credit Society]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-04	[Remitano - Cryptocurrency Exchange]	incransom	Link
2024-04-04	[mcalvain.com]	cactus	Link
2024-04-03	[Precision Pulley & Idler]	blacksuit	Link
2024-04-03	[Wacks Law Group]	qilin	Link
2024-04-03	[BeneCare Dental Insurance]	hunters	Link
2024-04-03	[Interface]	hunters	Link
2024-04-03	[DataBank]	hunters	Link
2024-04-03	[Beaver Run Resort]	hunters	Link
2024-04-03	[Benetton Group]	hunters	Link
2024-04-03	[Citi Trends]	hunters	Link
2024-04-03	[Intersport]	hunters	Link
2024-04-03	[West Idaho Orthopedics]	incransom	Link
2024-04-03	[Norman Urology Associates]	incransom	Link
2024-04-03	[Phillip Townsend Associates]	blacksuit	Link
2024-04-02	[San Pasqual Band of Mission Indians]	medusa	Link
2024-04-02	[East Baton Rouge Sheriff’s Office]	medusa	Link
2024-04-03	[Leicester City Council]	incransom	Link
2024-04-03	[Ringhoffer Verzahnungstechnik GmbH and Co. KG]	8base	Link
2024-04-03	[Samhwa Paint Ind. Ltd]	8base	Link
2024-04-03	[Tamura Corporation]	8base	Link
2024-04-03	[Apex Business Advisory]	8base	Link
2024-04-03	[Pim]	8base	Link
2024-04-03	[Innomotive Systems Hainichen GmbH]	raworld	Link
2024-04-03	[Seven Seas Technology]	rhysida	Link
2024-04-01	[casajove.com]	lockbit3	Link
2024-04-03	[delhipolice.gov.in]	killsec	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-02	[regencyfurniture.com]	cactus	Link
2024-04-02	[KICO GROUP]	raworld	Link
2024-04-02	[GRUPOCREATIVO HERRERA]	qilin	Link
2024-04-02	[Fincasrevuelta Data Leak]	everest	Link
2024-04-02	[Precision Pulley & Idler]	blacksuit	Link
2024-04-02	[W.P.J. McCarthy and Company]	qilin	Link
2024-04-02	[Crimsgroup Data Leak]	everest	Link
2024-04-02	[Gaia Herbs]	blacksuit	Link
2024-04-02	[Sterling Plumbing Inc]	raworld	Link
2024-04-02	[C&C Casa e Construção Ltda]	raworld	Link
2024-04-02	[TUBEX Aluminium Tubes]	raworld	Link
2024-04-01	[Roberson & Sons Insurance Services]	qilin	Link
2024-04-01	[Partridge Venture Engineering]	blacksuit	Link
2024-04-01	[anwaltskanzlei-kaufbeuren.de]	lockbit3	Link
2024-04-01	[pdq-airspares.co.uk]	blackbasta	Link
2024-04-01	[aerodynamicinc.com]	cactus	Link
2024-04-01	[besttrans.com]	cactus	Link
2024-04-01	[Xenwerx Initiatives, LLC]	incransom	Link
2024-04-01	[Blueline Associates]	incransom	Link
2024-04-01	[Sisu Healthcare]	incransom	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.