Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240409

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

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

—

Sicherheitsupdates für Ivanti: Schadcode kann durch VPN-Verbindungen schlüpfen

Es sind wichtige Sicherheitspatches für Ivanti Connect Secure und Policy Secure Gateways erschienen.

- Link

—

Cisco dichtet Schwachstellen in mehreren Produkten ab

Cisco hat zwölf Sicherheitsmitteilungen veröffentlicht. Die zugehörigen Updates dichten zahlreiche Sicherheitslücken ab.

- Link

—

Patchday Android: Angreifer können sich höhere Rechte verschaffen

Neben Google haben auch Samsung und weitere Hersteller wichtige Sicherheitsupdates für Androidgeräte veröffentlicht.

- Link

—

Kritische Sicherheitslücke in Wordpress-Plug-in Layerslider

IT-Forscher haben eine kritische Lücke im Wordpress-Plug-in Layerslider entdeckt. Es ist auf mehr als einer Million Seiten installiert.

- Link

—

Codeschmuggellücke in VMware SD-WAN Edge und Orchestrator

Drei Sicherheitslücken in VMwares SD-WAN Edge und Orchestrator ermöglichen Angreifern unter anderem, Schadcode einzuschleusen.

- Link

—

Google Chrome: Entwickler dichten drei Lücken ab, arbeiten an Cookie-Schutz

Im Webbrowser Chrome wurden drei Sicherheitslücken entdeckt. Google arbeitet zudem an Mechanismen gegen Cookie-Diebstahl.

- Link

—

Synology Surveillance Station: Mehrere Lücken gefährden Sicherheit

In der Software Surveillance Station von Synology klaffen Sicherheitslecks, die Angreifern etwa Codeschmuggel erlauben. Updates stopfen sie.

- 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	0.987440000	Link
CVE-2023-6553	0.916210000	0.988490000	Link
CVE-2023-5360	0.967230000	0.996410000	Link
CVE-2023-4966	0.964860000	0.995690000	Link
CVE-2023-47246	0.940270000	0.991120000	Link
CVE-2023-46805	0.964290000	0.995550000	Link
CVE-2023-46747	0.971350000	0.997820000	Link
CVE-2023-46604	0.973060000	0.998600000	Link
CVE-2023-43177	0.927670000	0.989790000	Link
CVE-2023-42793	0.970710000	0.997520000	Link
CVE-2023-39143	0.942940000	0.991470000	Link
CVE-2023-38646	0.928720000	0.989850000	Link
CVE-2023-38203	0.958450000	0.994090000	Link
CVE-2023-38035	0.973610000	0.998930000	Link
CVE-2023-36845	0.966640000	0.996240000	Link
CVE-2023-35813	0.905250000	0.987650000	Link
CVE-2023-3519	0.911860000	0.988190000	Link
CVE-2023-35082	0.950590000	0.992740000	Link
CVE-2023-35078	0.962310000	0.994950000	Link
CVE-2023-34993	0.944980000	0.991890000	Link
CVE-2023-34960	0.935410000	0.990580000	Link
CVE-2023-34634	0.925600000	0.989510000	Link
CVE-2023-34362	0.960290000	0.994490000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34039	0.907130000	0.987820000	Link
CVE-2023-3368	0.918440000	0.988730000	Link
CVE-2023-33246	0.973150000	0.998660000	Link
CVE-2023-32315	0.973840000	0.999060000	Link
CVE-2023-32235	0.911650000	0.988150000	Link
CVE-2023-30625	0.948330000	0.992430000	Link
CVE-2023-30013	0.956380000	0.993750000	Link
CVE-2023-29300	0.963460000	0.995270000	Link
CVE-2023-29298	0.926460000	0.989610000	Link
CVE-2023-28771	0.921620000	0.989010000	Link
CVE-2023-28432	0.943220000	0.991540000	Link
CVE-2023-28121	0.943690000	0.991610000	Link
CVE-2023-27524	0.972950000	0.998540000	Link
CVE-2023-27372	0.973490000	0.998880000	Link
CVE-2023-27350	0.972040000	0.998100000	Link
CVE-2023-26469	0.938630000	0.990930000	Link
CVE-2023-26360	0.963570000	0.995300000	Link
CVE-2023-26035	0.969280000	0.997030000	Link
CVE-2023-25717	0.957880000	0.993990000	Link
CVE-2023-25194	0.969270000	0.997020000	Link
CVE-2023-2479	0.963600000	0.995310000	Link
CVE-2023-24489	0.973810000	0.999040000	Link
CVE-2023-23752	0.952140000	0.992980000	Link
CVE-2023-23397	0.923530000	0.989210000	Link
CVE-2023-23333	0.963260000	0.995200000	Link
CVE-2023-22527	0.965680000	0.996020000	Link
CVE-2023-22518	0.969490000	0.997100000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-22515	0.971880000	0.998030000	Link
CVE-2023-21839	0.958450000	0.994090000	Link
CVE-2023-21554	0.959700000	0.994350000	Link
CVE-2023-20887	0.964080000	0.995470000	Link
CVE-2023-1671	0.965610000	0.996010000	Link
CVE-2023-0669	0.969030000	0.996950000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 08 Apr 2024

[UPDATE] [hoch] Node.js: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder seine Privilegien zu erweitern.

- Link

—

Mon, 08 Apr 2024

[UPDATE] [hoch] Ruby: Schwachstelle ermöglicht Manipulation von Dateien

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

- Link

—

Mon, 08 Apr 2024

[UPDATE] [hoch] OpenSSH: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Mon, 08 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

—

Mon, 08 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

—

Mon, 08 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

—

Mon, 08 Apr 2024

[UPDATE] [hoch] Adobe Magento: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Adobe Magento ausnutzen, um Cross-Site-Scripting (XSS)-Angriffe durchzuführen, Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.
- Link

—

Mon, 08 Apr 2024

[NEU] [hoch] IBM Personal Communications: Schwachstelle ermöglicht Privilegienerweiterung und Codeausführung mit den Rechten des Systems

Ein entfernter authentifizierter Angreifer kann eine Schwachstelle in IBM Personal Communications ausnutzen, um seine Privilegien zu erweitern und beliebigen Code mit den Rechten des Systems auszuführen.
- Link

—

Fri, 05 Apr 2024

[NEU] [hoch] Apache CloudStack: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache CloudStack ausnutzen, um die Authentifizierung zu umgehen, vertrauliche Informationen offenzulegen oder seine Privilegien zu erweitern und so die Kontrolle über das System zu übernehmen.
- Link

—

Fri, 05 Apr 2024

[NEU] [hoch] Apache HTTP Server: Mehrere Schwachstellen ermöglichen Manipulation von Daten

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um Daten zu manipulieren.

- Link

—

Fri, 05 Apr 2024

[NEU] [hoch] ESRI Portal for ArcGIS: Mehrere Schwachstellen

Ein entfernter authentifizierter Angreifer kann mehrere Schwachstellen in ESRI ArcGIS ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder Cross-Site Scripting (XSS)-Angriffe durchzuführen.

- Link

—

Fri, 05 Apr 2024

[NEU] [hoch] Broadcom Fabric OS: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Broadcom Fabric OS ausnutzen, um beliebigen Code auszuführen und um falsche Informationen darzustellen.

- Link

—

Fri, 05 Apr 2024

[NEU] [hoch] Dell ECS: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Dell ECS ausnutzen, um seine Privilegien zu erweitern, beliebigen Programmcode mit Administratorrechten auszuführen, Informationen offenzulegen, Dateien zu manipulieren, einen Cross-Site-Scripting-Angriff durchzuführen, Sicherheitsvorkehrungen zu umgehen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Fri, 05 Apr 2024

[UPDATE] [hoch] IBM DB2: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in IBM DB2 ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.

- Link

—

Fri, 05 Apr 2024

[UPDATE] [hoch] WordPress: Mehrere Schwachstellen

Ein entfernter authentifizierter Angreifer kann eine Schwachstelle in WordPress ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder beliebigen Code auszuführen.

- Link

—

Fri, 05 Apr 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 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

—

Fri, 05 Apr 2024

[UPDATE] [hoch] PostgreSQL JDBC Driver: Schwachstelle ermöglicht SQL-Injection

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PostgreSQL JDBC Driver ausnutzen, um eine SQL-Injection durchzuführen.

- Link

—

Fri, 05 Apr 2024

[UPDATE] [hoch] IBM MQ: Mehrere Schwachstellen

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

- Link

—

Fri, 05 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

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
4/8/2024	[EulerOS 2.0 SP9 : xorg-x11-server (EulerOS-SA-2024-1501)]	critical
4/8/2024	[EulerOS 2.0 SP9 : xorg-x11-server (EulerOS-SA-2024-1522)]	critical
4/8/2024	[EulerOS 2.0 SP9 : ghostscript (EulerOS-SA-2024-1505)]	critical
4/8/2024	[EulerOS 2.0 SP9 : ghostscript (EulerOS-SA-2024-1484)]	critical
4/9/2024	[EulerOS 2.0 SP9 : bind (EulerOS-SA-2024-1481)]	high
4/9/2024	[EulerOS 2.0 SP9 : unbound (EulerOS-SA-2024-1500)]	high
4/9/2024	[EulerOS 2.0 SP9 : shim (EulerOS-SA-2024-1497)]	high
4/9/2024	[EulerOS 2.0 SP9 : graphviz (EulerOS-SA-2024-1487)]	high
4/9/2024	[EulerOS 2.0 SP9 : sqlite (EulerOS-SA-2024-1498)]	high
4/8/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : go1.22 (SUSE-SU-2024:1121-1)]	high
4/8/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : go1.21 (SUSE-SU-2024:1122-1)]	high
4/8/2024	[SUSE SLES12 Security Update : squid (SUSE-SU-2024:1115-1)]	high
4/8/2024	[SUSE SLES15 / openSUSE 15 Security Update : squid (SUSE-SU-2024:1113-1)]	high
4/8/2024	[EulerOS 2.0 SP9 : binutils (EulerOS-SA-2024-1482)]	high
4/8/2024	[EulerOS 2.0 SP9 : python-pillow (EulerOS-SA-2024-1495)]	high
4/8/2024	[EulerOS 2.0 SP9 : gnutls (EulerOS-SA-2024-1507)]	high
4/8/2024	[EulerOS 2.0 SP9 : bind (EulerOS-SA-2024-1502)]	high
4/8/2024	[EulerOS 2.0 SP9 : graphviz (EulerOS-SA-2024-1508)]	high
4/8/2024	[EulerOS 2.0 SP9 : docker-runc (EulerOS-SA-2024-1504)]	high
4/8/2024	[EulerOS 2.0 SP9 : ncurses (EulerOS-SA-2024-1490)]	high
4/8/2024	[EulerOS 2.0 SP9 : python-pillow (EulerOS-SA-2024-1516)]	high
4/8/2024	[EulerOS 2.0 SP9 : gnutls (EulerOS-SA-2024-1486)]	high
4/8/2024	[EulerOS 2.0 SP9 : libxml2 (EulerOS-SA-2024-1489)]	high

Datum	Schwachstelle	Bewertung
4/8/2024	[EulerOS 2.0 SP9 : kernel (EulerOS-SA-2024-1509)]	high
4/8/2024	[EulerOS 2.0 SP9 : shim (EulerOS-SA-2024-1518)]	high
4/8/2024	[EulerOS 2.0 SP9 : docker-runc (EulerOS-SA-2024-1483)]	high
4/8/2024	[EulerOS 2.0 SP9 : kernel (EulerOS-SA-2024-1488)]	high
4/8/2024	[EulerOS 2.0 SP9 : giflib (EulerOS-SA-2024-1506)]	high
4/8/2024	[EulerOS 2.0 SP9 : binutils (EulerOS-SA-2024-1503)]	high
4/8/2024	[EulerOS 2.0 SP9 : giflib (EulerOS-SA-2024-1485)]	high
4/8/2024	[EulerOS 2.0 SP9 : unbound (EulerOS-SA-2024-1521)]	high
4/8/2024	[EulerOS 2.0 SP9 : sqlite (EulerOS-SA-2024-1519)]	high
4/8/2024	[EulerOS 2.0 SP9 : libxml2 (EulerOS-SA-2024-1510)]	high
4/8/2024	[EulerOS 2.0 SP9 : ncurses (EulerOS-SA-2024-1511)]	high
4/8/2024	[Oracle Linux 8 : nodejs:20 (ELSA-2024-1687)]	high
4/8/2024	[Oracle Linux 9 : less (ELSA-2024-1692)]	high
4/8/2024	[Oracle Linux 9 : nodejs:20 (ELSA-2024-1688)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“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

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 photo-thumbs.php Cross Site Scripting

DerbyNet version 9.0 suffers from a cross site scripting vulnerability in photo-thumbs.php.

- Link

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 checkin.php Cross Site Scripting

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

- Link

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 photo.php Cross Site Scripting

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

- Link

—

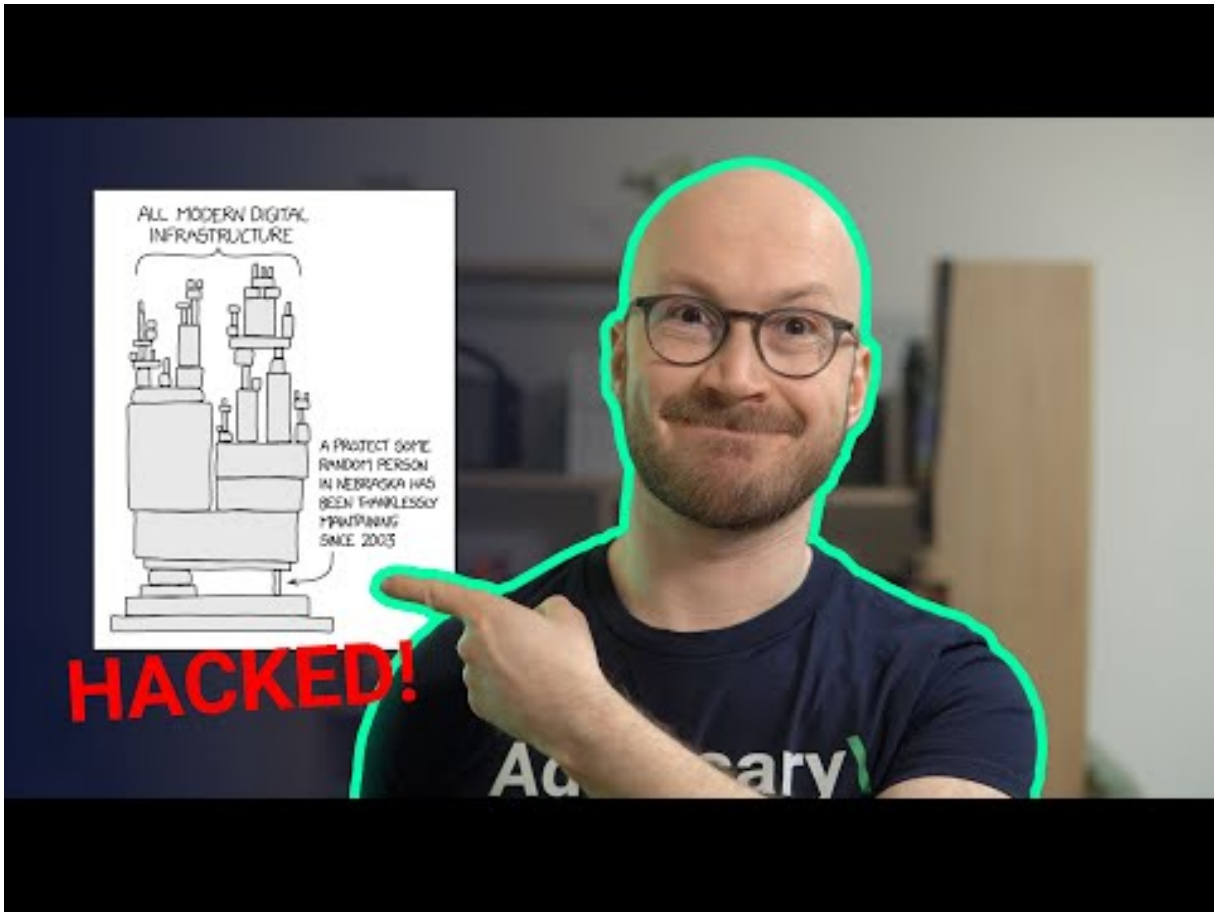
”

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
2024-04-07	CVS Group	[GBR]	Link
2024-04-07	St. Elisabeth-Stiftung	[DEU]	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
2024-04-09	[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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.