Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240430

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

Qnap schließt NAS-Sicherheitslücken aus Hacker-Wettbewerb Pwn2Own

NAS-Modelle von Qnap sind verwundbar. Nun hat der Hersteller Sicherheitsupdates für das Betriebssystem und Apps veröffentlicht.

- Link

—

Sicherheitsupdates: Angreifer können GitLab-Accounts übernehmen

Wichtige Sicherheitsupdates schließen mehrere Sicherheitslücken in GitLab. Der Anbieter rät zu einem zügigen Update.

- Link

—

Cross-Site Scripting: Sicherheitslücken in pfSense ermöglichen Admin-Cookieklau

Die Open-Source-Firewall pfSense hat mehrere Löcher, durch die Angreifer eigenen Javascript-Code einschleusen können. Updates sind verfügbar.

- Link

—

Cisco: Angreifer plazieren mithilfe neuer 0-Day-Lücke Hintertüren auf Firewalls

Zwei geschickt gestaltete Hintertüren auf Geräten mit Ciscos ASA- und FTD-System überleben Reboots und Systemupdates. Viele Details sind noch unklar.

- Link

—

AMD Radeon-Grafiktreiber: Update schließt Codeschmuggel-Lücke

AMD hat Updates für Radeon-Grafiktreiber für DirectX 11 veröffentlicht. Sie schließen Sicherheitslücken, durch die Angreifer Schadcode einschleusen können.

- Link

—

Jetzt patchen! Attacken auf Dateiübertragungsserver CrushFTP beobachtet

Angreifer haben Zugriff auf Systemdaten von CrushFTP-Servern. Verwundbare Systeme gibt es auch in Deutschland.

- Link

—

FIDO2-Sticks: Lücke in Yubikey-Verwaltungssoftware erlaubt Rechteausweitung

Um die FIDO2-Sticks von Yubikey zu verwalten, stellt der Hersteller eine Software bereit. Eine Lücke darin ermöglicht die Ausweitung der Rechte.

- Link

—

Mitel SIP-Phones anfällig für unbefugte Zugriffe

Mitel-SIP-Phones und -Konferenz-Produkte ermöglichen unbefugte Zugriffe und das Ausführen von Schadcode. Updates stehen bereit.

- Link

—

Update für Solarwinds FTP-Server Serv-U schließt Lücke mit hohem Risiko

Im Solarwinds Serv-U-FTP-Server klafft eine als hohes Risiko eingestufte Sicherheitslücke. Der Hersteller dichtet sie mit einem Update ab.

- Link

—

Jetzt patchen! Root-Attacken auf Cisco IMC können bevorstehen

Es sind wichtige Sicherheitsupdates für Cisco Integrated Management Controller und IOS erschienen. Exploitcode ist in Umlauf.

- 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	0.987630000	Link
CVE-2023-6553	0.916210000	0.988690000	Link
CVE-2023-5360	0.967230000	0.996480000	Link
CVE-2023-4966	0.966100000	0.996160000	Link
CVE-2023-49103	0.901710000	0.987640000	Link
CVE-2023-48795	0.939440000	0.991130000	Link
CVE-2023-47246	0.941130000	0.991340000	Link
CVE-2023-46805	0.965580000	0.996020000	Link
CVE-2023-46747	0.971350000	0.997930000	Link
CVE-2023-46604	0.972480000	0.998400000	Link
CVE-2023-43177	0.964020000	0.995530000	Link
CVE-2023-42793	0.971040000	0.997740000	Link
CVE-2023-39143	0.950730000	0.992940000	Link
CVE-2023-38646	0.913020000	0.988460000	Link
CVE-2023-38203	0.972020000	0.998170000	Link
CVE-2023-38035	0.973610000	0.998950000	Link
CVE-2023-36845	0.965540000	0.996020000	Link
CVE-2023-3519	0.911860000	0.988400000	Link
CVE-2023-35082	0.952190000	0.993150000	Link
CVE-2023-35078	0.966030000	0.996130000	Link
CVE-2023-34993	0.956820000	0.993960000	Link
CVE-2023-34960	0.938540000	0.991050000	Link
CVE-2023-34634	0.918830000	0.988940000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34362	0.955450000	0.993710000	Link
CVE-2023-34039	0.934640000	0.990590000	Link
CVE-2023-3368	0.918440000	0.988920000	Link
CVE-2023-33246	0.973120000	0.998690000	Link
CVE-2023-32315	0.974090000	0.999260000	Link
CVE-2023-32235	0.911650000	0.988380000	Link
CVE-2023-30625	0.945200000	0.992090000	Link
CVE-2023-30013	0.960350000	0.994610000	Link
CVE-2023-29300	0.970030000	0.997350000	Link
CVE-2023-29298	0.948030000	0.992460000	Link
CVE-2023-28771	0.921620000	0.989170000	Link
CVE-2023-28432	0.940320000	0.991250000	Link
CVE-2023-28121	0.945870000	0.992170000	Link
CVE-2023-27524	0.970780000	0.997650000	Link
CVE-2023-27372	0.973780000	0.999030000	Link
CVE-2023-27350	0.970720000	0.997620000	Link
CVE-2023-26469	0.933870000	0.990500000	Link
CVE-2023-26360	0.964040000	0.995530000	Link
CVE-2023-26035	0.969280000	0.997110000	Link
CVE-2023-25717	0.957880000	0.994140000	Link
CVE-2023-25194	0.969270000	0.997100000	Link
CVE-2023-2479	0.963600000	0.995390000	Link
CVE-2023-24489	0.974290000	0.999390000	Link
CVE-2023-23752	0.932080000	0.990290000	Link
CVE-2023-23397	0.926450000	0.989800000	Link
CVE-2023-23333	0.963260000	0.995300000	Link
CVE-2023-22527	0.974440000	0.999460000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-22518	0.966340000	0.996220000	Link
CVE-2023-22515	0.972060000	0.998180000	Link
CVE-2023-21839	0.958250000	0.994210000	Link
CVE-2023-21554	0.959160000	0.994390000	Link
CVE-2023-20887	0.961910000	0.994960000	Link
CVE-2023-20198	0.900800000	0.987580000	Link
CVE-2023-1671	0.967280000	0.996510000	Link
CVE-2023-0669	0.969750000	0.997250000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 29 Apr 2024

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

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

- Link

—

Mon, 29 Apr 2024

[NEU] [hoch] QNAP NAS: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in QNAP NAS ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.

- Link

—

Mon, 29 Apr 2024

[NEU] [hoch] win.rar WinRAR: Schwachstelle ermöglicht Denial of Service und Informationsoffenlegung

Ein Angreifer kann eine Schwachstelle in win.rar WinRAR ausnutzen, um einen Denial of Service Angriff durchzuführen oder vertrauliche Informationen offenlegen.

- Link

—

Mon, 29 Apr 2024

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

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

- Link

—

Mon, 29 Apr 2024

[NEU] [hoch] Hirschmann HiOS: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

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

- Link

—

Mon, 29 Apr 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

—

Mon, 29 Apr 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, 29 Apr 2024

[UPDATE] [hoch] Red Hat Enterprise Linux (shim): Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux in "shim" ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.

- Link

—

Fri, 26 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

—

Fri, 26 Apr 2024

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmaßnahmen zu umgehen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Fri, 26 Apr 2024

[UPDATE] [kritisch] CrushFTP: Schwachstelle ermöglicht Codeausführung mit administrativen Rechten

Ein entfernter Angreifer kann eine Schwachstelle in CrushFTP ausnutzen, um Code mit administrativen Rechten auszuführen

- Link

—

Fri, 26 Apr 2024

[UPDATE] [hoch] CODESYS: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in CODESYS ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder einen Brute-Force-Angriff durchzuführen.

- Link

—

Fri, 26 Apr 2024

[UPDATE] [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

—

Fri, 26 Apr 2024

[UPDATE] [hoch] HCL Domino Blog Template: Schwachstelle ermöglicht Codeausführung und Denial of Service

Ein entfernter anonymer Angreifer kann eine Schwachstelle im HCL Domino Blog Template ausnutzen, um beliebigen Code auszuführen oder einen Denial of Service zu verursachen.

- Link

—

Fri, 26 Apr 2024

[UPDATE] [hoch] Mehrere DNS Server: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in mehreren DNS Server Produkten ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Fri, 26 Apr 2024

[NEU] [UNGEPATCHT] [hoch] Red Hat Quay: Mehrere Schwachstellen ermöglichen Offenlegung von Informationen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat Quay ausnutzen, um Informationen offenzulegen.

- Link

—

Fri, 26 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

—

Fri, 26 Apr 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, seine Privilegien zu erweitern, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.

- Link

—

Fri, 26 Apr 2024

[UPDATE] [hoch] Red Hat Advanced Cluster Management for Kubernetes: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen im Red Hat Advanced Cluster Management for Kubernetes ausnutzen, um einen Denial of Service Angriff durchzuführen oder beliebigen Code auszuführen.

- Link

—

Fri, 26 Apr 2024

[UPDATE] [hoch] Mozilla Firefox, Firefox ESR und Thunderbird: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, seine Privilegien zu erweitern oder einen nicht spezifizierten Angriff durchzuführen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
4/29/2024	[Fedora 40 : libuev (2024-40fbf3ee48)]	critical
4/29/2024	[Fedora 40 : openexr (2024-55247f3a4f)]	critical
4/29/2024	[Fedora 40 : mingw-qt6-qt3d / mingw-qt6-qt5compat / mingw-qt6-qtactiveqt / etc (2024-7f2064f068)]	critical
4/29/2024	[Fedora 37 : pypy3.9 (2023-af5206f71d)]	critical
4/29/2024	[Fedora 37 : mbedtls (2023-7456a62f60)]	critical
4/29/2024	[Fedora 40 : python2.7 (2023-de99cdb793)]	critical
4/29/2024	[NextChat < 2.11.3 SSRF]	critical
4/29/2024	[NextChat < 2.11.3 SSRF]	critical
4/29/2024	[Amazon Linux AMI : xorg-x11-server (ALAS-2024-1932)]	critical
4/29/2024	[Ubuntu 24.04 LTS. : FreeRDP vulnerabilities (USN-6759-1)]	critical
4/29/2024	[Fedora 40 : iwd (2024-3fa713f2e0)]	high
4/29/2024	[Fedora 40 : python-cryptography (2024-9d2de2b051)]	high
4/29/2024	[Fedora 40 : libvirt-sandbox (2024-ebf015aa4e)]	high
4/29/2024	[Fedora 40 : grub2 (2024-2b545d3085)]	high
4/29/2024	[Fedora 40 : oggvideotools (2023-9f6281eaf7)]	high
4/29/2024	[Fedora 40 : httpd (2024-937be154d8)]	high
4/29/2024	[Fedora 37 : yarnpkg (2023-8d4b772755)]	high
4/29/2024	[Fedora 40 : pypy (2023-6000e06581)]	high
4/29/2024	[Fedora 40 : firefox (2024-cd3a64f43b)]	high
4/29/2024	[Fedora 40 : iwd / libell (2024-58c59bfa4c)]	high
4/29/2024	[Fedora 40 : rubygem-actioncable / rubygem-actionmailbox / rubygem-actionmailer / etc (2023-28962dd58a)]	high
4/29/2024	[Fedora 40 : trafficserver (2024-111a8a624b)]	high
4/29/2024	[Fedora 40 : golang-gvisor (2024-80e062d21a)]	high
4/29/2024	[Fedora 40 : flatpak (2024-43ea98691e)]	high

Datum	Schwachstelle	Bewertung
4/29/2024	[Fedora 40 : ceph (2024-1c5e37820f)]	high
4/29/2024	[Amazon Linux AMI : httpd24 (ALAS-2024-1931)]	high
4/29/2024	[Amazon Linux AMI : glibc (ALAS-2024-1930)]	high
4/29/2024	[Ubuntu 24.04 LTS. : GNU C Library vulnerability (USN-6737-2)]	high
4/29/2024	[Ubuntu 24.04 LTS. : Apache HTTP Server vulnerabilities (USN-6729-3)]	high
4/29/2024	[Oracle Linux 7 : tigervnc (ELSA-2024-2080)]	high
4/29/2024	[Oracle Linux 8 : container-tools:4.0 (ELSA-2024-2084)]	high
4/29/2024	[CentOS 8 : firefox (CESA-2024:1912)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

"Mon, 29 Apr 2024
Kemp LoadMaster Unauthenticated Command Injection
This Metasploit module exploits an unauthenticated command injection vulnerability in Progress Kemp LoadMaster in the authorization header after version 7.2.48.1. The following versions are patched: 7.2.59.2 (GA), 7.2.54.8 (LTSF), and 7.2.48.10 (LTS).
- Link
—
" "Mon, 29 Apr 2024
Doctor Appointment Management System 1.0 Cross Site Scripting
Doctor Appointment Management System version 1.0 suffers from a cross site scripting vulnerability.
- Link
—
" "Mon, 29 Apr 2024
ESET NOD32 Antivirus 17.1.11.0 Unquoted Service Path
ESET NOD32 Antivirus version 17.1.11.0 suffers from an unquoted service path vulnerability.
- Link
—

" "Thu, 25 Apr 2024

PowerVR PMRMMapPMR() Writability Check

PowerVR has a security issue where a writability check in PMRMMapPMR() does not clear VM_MAYWRITE.

- Link

—

" "Wed, 24 Apr 2024

Apache Solr Backup/Restore API Remote Code Execution

Apache Solr versions 6.0.0 through 8.11.2 and versions 9.0.0 up to 9.4.1 are affected by an unrestricted file upload vulnerability which can result in remote code execution in the context of the user running Apache Solr. When Apache Solr creates a Collection, it will use a specific directory as the classpath and load some classes from it. The backup function of the Collection can export malicious class files uploaded by attackers to the directory, allowing Solr to load custom classes and create arbitrary Java code. Execution can further bypass the Java sandbox configured by Solr, ultimately causing arbitrary command execution.

- Link

—

" "Wed, 24 Apr 2024

Relate Learning And Teaching System SSTI / Remote Code Execution

Relate Learning and Teaching System versions prior to 2024.1 suffers from a server-side template injection vulnerability that leads to remote code execution. This particular finding targets the Batch-Issue Exam Tickets function.

- Link

—

" "Wed, 24 Apr 2024

Nginx 1.25.5 Host Header Validation

Nginx versions 1.25.5 and below appear to have a host header filtering validation bug that could possibly be used for malice.

- Link

—

" "Tue, 23 Apr 2024

FortiNet FortiClient EMS 7.2.2 / 7.0.10 SQL Injection / Remote Code Execution

A remote SQL injection vulnerability exists in FortiNet FortiClient EMS (Endpoint Management Server) versions 7.2.0 through 7.2.2 and 7.0.1 through 7.0.10. FortiClient EMS serves as an endpoint management solution tailored for enterprises, offering a centralized platform for overseeing enrolled endpoints. The SQL injection vulnerability is due to user controller strings which can be sent directly into database queries. FcmDaemon.exe is the main service responsible for communicating with enrolled clients. By default it listens on port 8013 and communicates with FCTDas.exe which is

responsible for translating requests and sending them to the database. In the message header of a specific request sent between the two services, the FCTUID parameter is vulnerable to SQL injection. It can be used to enable the xp_cmdshell which can then be used to obtain unauthenticated remote code execution in the context of NT AUTHORITY\SYSTEM. Upgrading to either 7.2.3, 7.0.11 or above is recommended by FortiNet. It should be noted that in order to be vulnerable, at least one endpoint needs to be enrolled / managed by FortiClient EMS for the necessary vulnerable services to be available.

- Link

—

" "Tue, 23 Apr 2024

GitLens Git Local Configuration Execution

GitKraken GitLens versions prior to 14.0.0 allow an untrusted workspace to execute git commands. A repo may include its own .git folder including a malicious config file to execute arbitrary code. Tested against VSCode 1.87.2 with GitLens 13.6.0 on Ubuntu 22.04 and Windows 10.

- Link

—

" "Tue, 23 Apr 2024

Visual Studio Code Execution

This Metasploit module creates a vsix file which can be installed in Visual Studio Code as an extension. At activation/install, the extension will execute a shell or two. Tested against VSCode 1.87.2 on Ubuntu 22.04.

- Link

—

" "Tue, 23 Apr 2024

Gambio Online Webshop 4.9.2.0 Remote Code Execution

A remote code execution vulnerability in Gambio online webshop versions 4.9.2.0 and below allows remote attackers to run arbitrary commands via an unauthenticated HTTP POST request. The identified vulnerability within Gambio pertains to an insecure deserialization flaw, which ultimately allows an attacker to execute remote code on affected systems. The insecure deserialization vulnerability in Gambio poses a significant risk to affected systems. As it allows remote code execution, adversaries could exploit this flaw to execute arbitrary commands, potentially resulting in complete system compromise, data exfiltration, or unauthorized access to sensitive information.

- Link

—

" "Tue, 23 Apr 2024

Palo Alto Networks PAN-OS Unauthenticated Remote Code Execution

This Metasploit module exploits two vulnerabilities in Palo Alto Networks PAN-OS that allow an unauthenticated attacker to create arbitrarily named files and execute shell commands. Configuration

requirements are PAN-OS with GlobalProtect Gateway or GlobalProtect Portal enabled and telemetry collection on (default). Multiple versions are affected. Payloads may take up to one hour to execute, depending on how often the telemetry service is set to run.

- Link

—

" "Tue, 23 Apr 2024

Palo Alto PAN-OS Command Execution / Arbitrary File Creation

Palo Alto PAN-OS versions prior to 11.1.2-h3 command injection and arbitrary file creation exploit.

- Link

—

" "Mon, 22 Apr 2024

LRMS PHP 1.0 SQL Injection / Shell Upload

LRMS PHP version 1.0 suffers from remote shell upload and multiple remote SQL injection vulnerabilities.

- Link

—

" "Mon, 22 Apr 2024

Dreamehome 2.1.5 Broken Authorization

Dreamehome versions 2.1.5 and below suffer from multiple broken authorization vulnerabilities.

- Link

—

" "Mon, 22 Apr 2024

SofaWiki 3.9.2 Shell Upload

SofaWiki version 3.9.2 suffers from a remote shell upload vulnerability.

- Link

—

" "Mon, 22 Apr 2024

Laravel Framework 11 Credential Disclosure

Laravel Framework version 11 suffers from a credential disclosure vulnerability.

- Link

—

" "Fri, 19 Apr 2024

FlatPress 1.3 Shell Upload

FlatPress version 1.3 suffers from a remote shell upload vulnerability.

- Link

—

" "Fri, 19 Apr 2024

MindManager Local Privilege Escalation

MindManager suffers from a local privilege escalation vulnerability via MSI installer Repair Mode.

- Link

—

" "Fri, 19 Apr 2024

WordPress Background Image Cropper 1.2 Shell Upload

WordPress Background Image Cropper plugin version 1.2 suffers from a remote shell upload vulnerability.

- Link

—

" "Fri, 19 Apr 2024

Flowise 1.6.5 Authentication Bypass

Flowise version 1.6.5 suffers from an authentication bypass vulnerability.

- Link

—

" "Fri, 19 Apr 2024

Relate Learning And Teaching System SSTI / Remote Code Execution

Relate Learning and Teaching System versions prior to 2024.1 suffers from a server-side template injection vulnerability that leads to remote code execution. This particular finding targets the Markup Sandbox function.

- Link

—

" "Thu, 18 Apr 2024

Elber Wayber Analog/Digital Audio STL 4.00 Insecure Direct Object Reference

Elber Wayber Analog/Digital Audio STL version 4.00 suffers from an unauthenticated device configuration and client-side hidden functionality disclosure vulnerability.

- Link

—

" "Thu, 18 Apr 2024

Elber Wayber Analog/Digital Audio STL 4.00 Authentication Bypass

Elber Wayber Analog/Digital Audio STL version 4.00 suffers from an authentication bypass vulnerability through a direct and unauthorized access to the password management functionality. The issue allows attackers to bypass authentication by manipulating the set_pwd endpoint that enables them to overwrite the password of any user within the system. This grants unauthorized and administrative access to protected areas of the application compromising the device's system security.suffers from a bypass vulnerability.

- Link

—

" "Thu, 18 Apr 2024

Elber ESE DVB-S/S2 Satellite Receiver 1.5.x Insecure Direct Object Reference

Elber ESE DVB-S/S2 Satellite Receiver version 1.5.x suffers from an unauthenticated device configuration and client-side hidden functionality disclosure vulnerability.

- Link

—

"

4.2 0-Days der letzten 5 Tage

"Mon, 29 Apr 2024

ZDI-24-416: Centreon sysName Cross-Site Scripting Remote Code Execution Vulnerability

- Link

—

" "Fri, 26 Apr 2024

ZDI-24-415: (Pwn2Own) Oracle VirtualBox E1000 Uninitialized Memory Information Disclosure Vulnerability

- Link

—

" "Fri, 26 Apr 2024

ZDI-24-414: (Pwn2Own) Oracle VirtualBox AHCI Controller Uninitialized Memory Information Disclosure Vulnerability

- Link

—

" "Fri, 26 Apr 2024

ZDI-24-413: (Pwn2Own) Oracle VirtualBox DevVGA Out-Of-Bounds Write Local Privilege Escalation Vulnerability

- Link

—

" "Fri, 26 Apr 2024

ZDI-24-412: (Pwn2Own) Oracle VirtualBox VirtIOCore Buffer Overflow Local Privilege Escalation Vulnerability

- Link

—

" "Fri, 26 Apr 2024

ZDI-24-411: (Pwn2Own) Oracle VirtualBox BusLogic Uninitialized Memory Information Disclosure Vulnerability

- Link

—

" "Fri, 26 Apr 2024

ZDI-24-410: Oracle VirtualBox vboxdrv Improper Privilege Management Local Privilege Escalation Vulnerability

- Link

—

" "Fri, 26 Apr 2024

ZDI-24-409: Oracle VirtualBox Guest Additions Improper Access Control Local Privilege Escalation Vulnerability

- Link

—

" "Fri, 26 Apr 2024

ZDI-24-408: Oracle VirtualBox Web Service Exposure of Resource to Wrong Sphere Information Disclosure Vulnerability

- Link

—

" "Fri, 26 Apr 2024

ZDI-24-407: X.Org Server ProcRenderAddGlyphs Use-After-Free Local Privilege Escalation Vulnerability

- Link

—

" "Fri, 26 Apr 2024

ZDI-24-406: Adobe After Effects AEP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

" "Fri, 26 Apr 2024

ZDI-24-405: Lexmark CX331adwe IPP Server Authorization HTTP Header Heap-Based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

"

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Oh wow, this was *very* close: xz-utils was backdoored ⬚
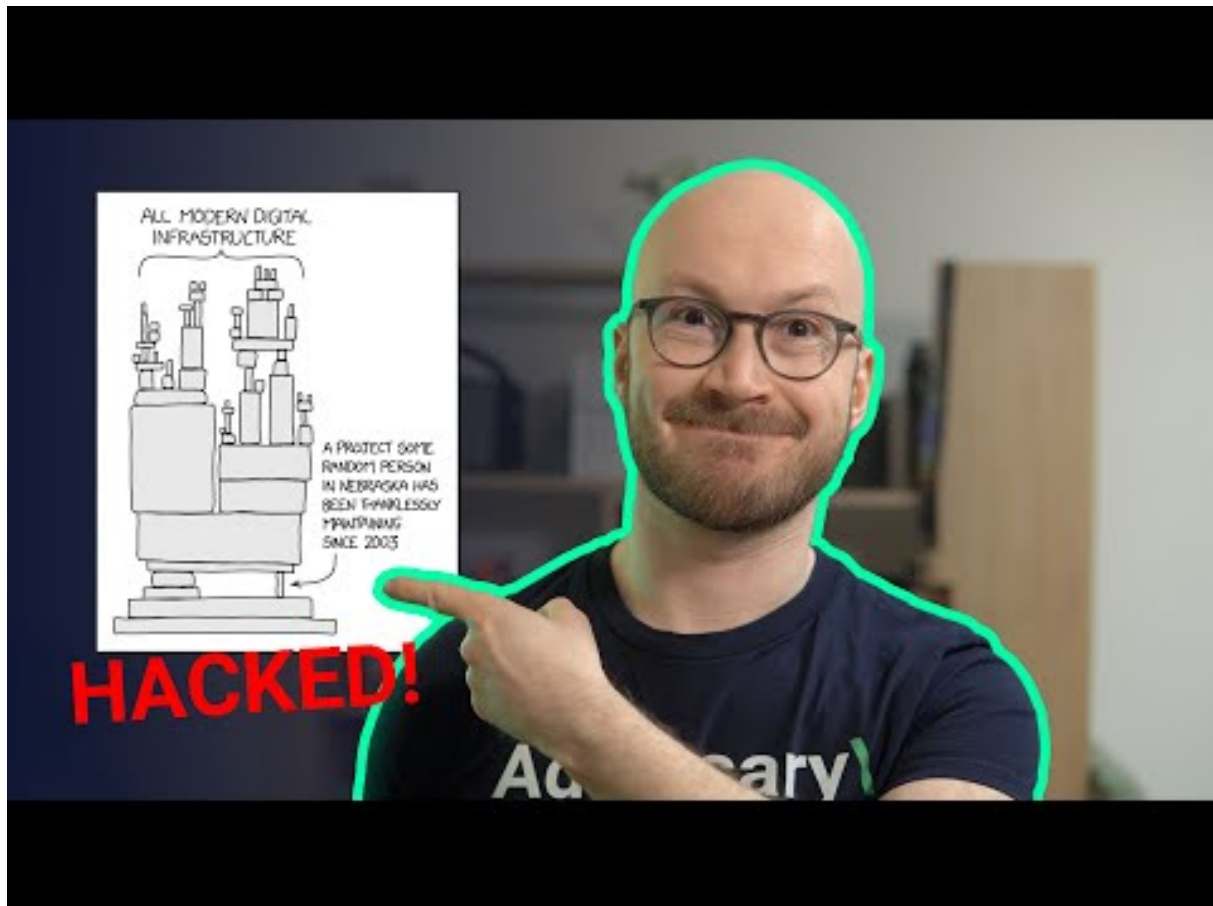
Zum Youtube Video

6 Cyberangriffe: (Apr)

Datum	Opfer	Land	Information
2024-04-25	Ville de Gravelines	[FRA]	Link
2024-04-25	Kansas City Scout	[USA]	Link
2024-04-23	Skanlog	[SWE]	Link
2024-04-23	Municipalité de La Guadeloupe	[CAN]	Link
2024-04-22	Ville d'Albi	[FRA]	Link
2024-04-20	🯄🯄🯄🯄 (Union Hospital)	[HKG]	Link
2024-04-20	Coppel	[MEX]	Link
2024-04-20	Petit commerce à Bad Wörishofen	[DEU]	Link
2024-04-19	Swisspro	[CHE]	Link
2024-04-19	Ordre des infirmières et infirmiers du Québec (OIIQ)	[CAN]	Link
2024-04-18	Synlab	[ITA]	Link
2024-04-18	Floirac	[FRA]	Link
2024-04-18	Carpetright	[GBR]	Link
2024-04-17	Legislative Bill Drafting Commission	[USA]	Link
2024-04-17	Écoles du comté de Glynn	[USA]	Link
2024-04-17	Barnett's Couriers	[AUS]	Link
2024-04-16	Hôpital Simone Veil à Cannes	[FRA]	Link
2024-04-16	Norrmjerier	[SWE]	Link
2024-04-16	Vooruit.brussels	[BEL]	Link
2024-04-15	Le Slip Français	[FRA]	Link
2024-04-15	Octapharma Plasma	[USA]	Link
2024-04-15	Police Fédérale du Brésil	[BRA]	Link
2024-04-15	Comté de Coffee, Géorgie	[USA]	Link
2024-04-14	Plus Servicios	[CHL]	Link
2024-04-14	Frontier Communications	[USA]	Link

Datum	Opfer	Land	Information
2024-04-14	Le ministère de la Santé de la République Dominicaine.	[DOM]	Link
2024-04-13	Tyler Technologies	[USA]	Link
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
2024-04-10	The de Ferrers Trust	[GBR]	Link
2024-04-09	The Heritage Foundation	[USA]	Link
2024-04-09	Pak Suzuki	[PAK]	Link
2024-04-09	Extern	[IRL]	Link
2024-04-09	Speedy France	[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
2024-04-04	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
2024-04-29	[ch-cannes.fr]	lockbit3	Link
2024-04-29	[Mellitah Oil & Gas / Enigas Ly (Eni Electricity, Oil & Gas)]	ransomhub	Link
2024-04-29	[Lumina Americas]	8base	Link
2024-04-29	[The Line Up, Inc]	8base	Link
2024-04-29	[Medizinische Grosshandlung GmbH]	8base	Link
2024-04-26	[Thinkadam]	spacebears	Link
2024-04-28	[CORTEX Chiropractic & Clinical Neuroscience]	spacebears	Link
2024-04-28	[todoagro]	spacebears	Link
2024-04-26	[Mr Bean]	spacebears	Link
2024-04-25	[SM EMBALLAGE]	spacebears	Link
2024-04-25	[Surewerx USA]	spacebears	Link
2024-04-27	[Fifisystems]	spacebears	Link
2024-04-27	[Fliesenstudio am Rhein]	spacebears	Link
2024-04-26	[hospitalescultural.com.br]	qiulong	Link
2024-04-28	[Magicolor]	hunters	Link
2024-04-27	[Herron Todd White]	blacksuit	Link
2024-04-27	[Human Technology Inc.]	incransom	Link
2024-04-25	[Anders Group]	medusa	Link
2024-04-27	[polaris-SOLUCIONES TECNOLÓGICAS PARA EMPRESAS – polaris.es]	ransomhub	Link
2024-04-26	[iddink.nl]	cactus	Link
2024-04-27	[thelawrencegroup.com_privat]	blackbasta	Link
2024-04-26	[Axip Energy Services]	play	Link
2024-04-26	[sesenergy.org]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-26	[Original Herkimer Cheese]	play	Link
2024-04-26	[Precision Fluid Controls]	play	Link
2024-04-26	[Yale Mortgage]	play	Link
2024-04-26	[Madata]	play	Link
2024-04-26	[Legislative Bill Drafting Commission]	play	Link
2024-04-26	[Toolmarts]	play	Link
2024-04-26	[New Hudson Facades]	play	Link
2024-04-26	[sandipuniversity.edu.in]	darkvault	Link
2024-04-26	[SSS Australia]	hunters	Link
2024-04-26	[Rocky Mountain Sales]	hunters	Link
2024-04-26	[Erler & Kalinowski]	dAn0n	Link
2024-04-26	[CDSHotels]	rhysida	Link
2024-04-26	[Precision Time Systems]	ransomhub	Link
2024-04-26	[Jutebag]	ransomhub	Link
2024-04-25	[Protected: HIDE NAME SELL DATA SOON]	medusalocker	Link
2024-04-25	[atriline.by]	darkvault	Link
2024-04-02	[United Equitable Group]	dAn0n	Link
2024-04-10	[Allen Blasting and Coating]	dAn0n	Link
2024-04-11	[Semilab]	dAn0n	Link
2024-04-15	[O'Connell Mahon Architects]	dAn0n	Link
2024-04-25	[Les Miroirs St-Antoine Inc]	everest	Link
2024-04-25	[Design Intoto]	ransomhub	Link
2024-04-25	[Beloinlaw]	qilin	Link
2024-04-24	[bzrastreador.com.br]	darkvault	Link
2024-04-25	[Peter Condakes]	blacksuit	Link
2024-04-24	[hominemclinic.com.br]	qiulong	Link
2024-04-24	[Central Power Systems and Services]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-24	[Mainwein]	raworld	Link
2024-04-14	[Army Welfare Trust]	ransomhouse	Link
2024-04-23	[The Council of Fashion Designers of America]	medusa	Link
2024-04-23	[Principle Cleaning Services]	medusa	Link
2024-04-24	[EUROPEANPROF - Expertos en Seguridad y Altura -]	ransomhub	Link
2024-04-24	[true.co.uk]	blackbasta	Link
2024-04-24	[CORIENT]	ransomhub	Link
2024-04-24	[[Published]Constelacion Savings and Credit Society]	ransomhub	Link
2024-04-24	[https://goftac.com/ firsttx.com First Texas Alliance Corp (FTAC)]	alphalocker	Link
2024-04-23	[www.drwilliansegalin.com.br]	qiulong	Link
2024-04-23	[Octapharma Plasma]	blacksuit	Link
2024-04-23	[Ministerio de Desarrollo Local]	rhysida	Link
2024-04-23	[rangam.com]	abyss	Link
2024-04-23	[defi SOLUTIONS.]	bianlian	Link
2024-04-23	[ghimli.com]	cactus	Link
2024-04-22	[draandrearechia.com.br]	qiulong	Link
2024-04-05	[www.trifecta.com]	apt73	Link
2024-04-22	[jean-nouvel]	qilin	Link
2024-04-22	[HARMAN - CYNC SOLUTIONS client]	ransomhub	Link
2024-04-19	[saglobal.com]	cactus	Link
2024-04-19	[concordegroup.ca]	cactus	Link
2024-04-19	[ebir.com]	cactus	Link
2024-04-19	[coastalcargogroup.com]	cactus	Link
2024-04-22	[Texas Retina Associates]	bianlian	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-22	[Wasserkraft Volk AG]	8base	Link
2024-04-22	[Speedy France]	8base	Link
2024-04-22	[The Tech Interactive]	8base	Link
2024-04-22	[Bieler + Lang GmbH]	8base	Link
2024-04-22	[FEB31st]	8base	Link
2024-04-17	[Asteco]	ransomexx	Link
2024-04-22	[D'amico & Pettinicchi, LLC]	bianlian	Link
2024-04-22	[Optometric Physicians of Middle Tennessee]	bianlian	Link
2024-04-19	[www.rosalvoautomoveis.com.br]	qiulong	Link
2024-04-19	[www.drlincoln.com.br]	qiulong	Link
2024-04-22	[charlesparsons (Attack again)]	raworld	Link
2024-04-20	[Ted Brown Music]	medusa	Link
2024-04-17	[mulfordconstruction.com]	embargo	Link
2024-04-18	[taylorlaw.net]	lockbit3	Link
2024-04-18	[NORTHEAST OHIO NEIGHBORHOOD HEALTH SERVICES (NEON)]	medusa	Link
2024-04-20	[Continuing Healthcare Solutions]	incransom	Link
2024-04-20	[Lutheran Social Services of Indiana]	incransom	Link
2024-04-19	[kjf-augsburg.de]	lockbit3	Link
2024-04-19	[eurosko.com]	lockbit3	Link
2024-04-19	[CYNC SOLUTIONS - The unexpected target.]	ransomhub	Link
2024-04-19	[Targus.com]	redransomware	Link
2024-04-19	[The law firm Dr. Fingerle Rechtsanwälte]	qilin	Link
2024-04-19	[call4health.com]	lockbit3	Link
2024-04-19	[tascoplumbing.com]	lockbit3	Link
2024-04-19	[fluenthome.com]	blackbasta	Link
2024-04-19	[macphie.com]	blackbasta	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-19	[cavotec.com]	blackbasta	Link
2024-04-19	[hymer-alu.de]	blackbasta	Link
2024-04-19	[azdel.com]	blackbasta	Link
2024-04-06	[amctheatres.com]	dispossessor	Link
2024-04-18	[navalaviationmuseum.org]	dispossessor	Link
2024-04-18	[nationalflightacademy.com]	dispossessor	Link
2024-04-19	[Hey everyone! Some private keys here.]	hellogookie	Link
2024-04-19	[Hey cisco!]	hellogookie	Link
2024-04-19	[CD Projekt!]	hellogookie	Link
2024-04-19	[sierraconstruction.ca]	lockbit3	Link
2024-04-19	[Alltruck Bodies]	play	Link
2024-04-19	[SIS Automatisering]	play	Link
2024-04-19	[Pennsylvania Convention Center]	play	Link
2024-04-19	[Engineered Automation of Maine]	play	Link
2024-04-19	[JE Owens]	play	Link
2024-04-19	[P??????? & ????]	play	Link
2024-04-18	[Mid-South Health Systems]	hunters	Link
2024-04-18	[etateam.be]	qilin	Link
2024-04-18	[dc.gov]	lockbit3	Link
2024-04-18	[JE Owens & Company PA.]	bianlian	Link
2024-04-18	[Western Saw Inc.]	bianlian	Link
2024-04-18	[Myers Automotive Group]	akira	Link
2024-04-18	[xdconnects.com]	cactus	Link
2024-04-18	[sagaciousresearch.com]	lockbit3	Link
2024-04-18	[ablinc.com]	lockbit3	Link
2024-04-18	[ht-hospitaltechnik.de]	blackout	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-18	[Mercatino S.r.l. https://www.mercatinousato.com/]	ransomhub	Link
2024-04-18	[Precision Pulley & Idler]	blacksuit	Link
2024-04-18	[https://geodis.com]	alphalocker	Link
2024-04-18	[FábricaInfo]	ransomhub	Link
2024-04-17	[doyon.com	doyondrilling.co	blackbasta
2024-04-17	[Mercatino https://www.mercatinousato.com/]	ransomhub	Link
2024-04-17	[Delano Joint Union High School District]	incransom	Link
2024-04-17	[Serfilco, RP Adams, Baron Blakeslee, Pacer, Service Filtration of Canada, Polymar.]	akira	Link
2024-04-17	[tristatetruckandequip.com]	lockbit3	Link
2024-04-17	[craigwire.com]	lockbit3	Link
2024-04-17	[Lee University]	medusa	Link
2024-04-17	[TrueNet Communications Corp]	ciphbit	Link
2024-04-17	[drmarbys.com]	cactus	Link
2024-04-17	[rehab.ie]	lockbit3	Link
2024-04-17	[D&V Electronics]	blacksuit	Link
2024-04-17	[Len Dubois Trucking]	bianlian	Link
2024-04-17	[Pioneer Oil Company, Inc.]	bianlian	Link
2024-04-16	[Empresa de energía del Bajo Putumayo]	ransomhub	Link
2024-04-16	[Change HealthCare - OPTUM Group - United HealthCare Group - FOR SALE]	ransomhub	Link
2024-04-16	[UPC Technology Corporation]	blacksuit	Link
2024-04-16	[Wright Brothers Construction]	akira	Link
2024-04-16	[Medequip Assistive Technology]	akira	Link
2024-04-16	[hbmolding.com]	lockbit3	Link
2024-04-16	[Lotz Trucking]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-16	[Studio LAMBDA]	akira	Link
2024-04-16	[City of St. Cloud, Florida]	hunters	Link
2024-04-16	[Grupo Cuevas]	ransomhub	Link
2024-04-16	[The Royal Family of Great Britain]	snatch	Link
2024-04-15	[Thermodyn Corporation]	medusa	Link
2024-04-16	[[UPDATE] Robeson County Sheriff's Office]	ransomhub	Link
2024-04-16	[St. Cloud Florida]	hunters	Link
2024-04-16	[UnivationTechnologies]	raworld	Link
2024-04-16	[Autoglass]	raworld	Link
2024-04-16	[charlesparsons]	raworld	Link
2024-04-16	[Cembell Industries]	qilin	Link
2024-04-12	[Heritage Cooperative]	play	Link
2024-04-15	[Druckman Law Group]	incransom	Link
2024-04-15	[Pulaski academy]	incransom	Link
2024-04-15	[Chicony Electronics]	hunters	Link
2024-04-15	[Fullington Trailways]	dragonforce	Link
2024-04-15	[bigtoe.yoga]	darkvault	Link
2024-04-15	[regulatormarine.com]	cactus	Link
2024-04-15	[jeyesfluid.co.uk]	lockbit3	Link
2024-04-15	[Deacon Jones]	dragonforce	Link
2024-04-15	[Biggs Cardosa Associates]	blacksuit	Link
2024-04-15	[The Post and Courier]	blacksuit	Link
2024-04-15	[Best Reward Federal Credit Union]	akira	Link
2024-04-15	[LYON TERMINAL]	8base	Link
2024-04-15	[R.B. Woodcraft, Inc.]	8base	Link
2024-04-15	[GPI Corporate]	8base	Link
2024-04-15	[SOA Architecture]	8base	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-15	[ASMFC: Atlantic States Marine Fisheries Commission]	8base	Link
2024-04-15	[The Souza Agency Inc.]	8base	Link
2024-04-15	[LEMODOR]	8base	Link
2024-04-15	[Council for Relationships]	8base	Link
2024-04-15	[compagniedephalsbourg.com]	threeam	Link
2024-04-15	[ndpaper.com]	lockbit3	Link
2024-04-14	[qint.com.br]	darkvault	Link
2024-04-14	[Jack Doheny Company]	hunters	Link
2024-04-13	[Traverse City Area Public Schools]	medusa	Link
2024-04-14	[Omni Hotels & Resorts (US)]	daixin	Link
2024-04-13	[countryvillahealth.com]	lockbit3	Link
2024-04-13	[disb.dc.gov]	lockbit3	Link
2024-04-09	[Williams County Abstract Company]	medusa	Link
2024-04-12	[Solano County Library]	medusa	Link
2024-04-12	[Alliance Mercantile]	medusa	Link
2024-04-12	[Novus International]	medusa	Link
2024-04-13	[Toyota Brazil]	hunters	Link
2024-04-13	[Kablutronik SRL]	hunters	Link
2024-04-13	[Caxton and CTP Publishers and Printers]	hunters	Link
2024-04-13	[NanoLumens]	hunters	Link
2024-04-13	[Integrated Control]	hunters	Link
2024-04-13	[Frederick Wildman and Sons]	hunters	Link
2024-04-12	[oraclecms.com]	lockbit3	Link
2024-04-04	[thsp.co.uk]	darkvault	Link
2024-04-12	[tommyclub.co.uk]	darkvault	Link
2024-04-12	[Notions Marketing]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-12	[Jordano's Inc.]	hunters	Link
2024-04-12	[Bojangles' International]	hunters	Link
2024-04-12	[Snchez-Betances Sifre & Muñoz-Noya]	akira	Link
2024-04-10	[Feldstein & Stewart]	play	Link
2024-04-12	[Agate Construction]	play	Link
2024-04-12	[H??????? C??????????]	play	Link
2024-04-12	[Robeson County Sheriff's Office]	ransomhub	Link
2024-04-12	[MCP GROUP Commercial Contractor Topeka]	blacksuit	Link
2024-04-12	[Hernando County]	rhysida	Link
2024-04-11	[baheyabeauty.com]	darkvault	Link
2024-04-11	[baheya.com]	darkvault	Link
2024-04-12	[Oki Golf]	rhysida	Link
2024-04-12	[Gimex]	raworld	Link
2024-04-12	[Victor Fauconnier]	raworld	Link
2024-04-11	[MoldTech]	play	Link
2024-04-11	[Theatrixx Technologies]	play	Link
2024-04-11	[Access Intelligence]	play	Link
2024-04-11	[New England Wooden Ware]	play	Link
2024-04-11	[LS Networks]	play	Link
2024-04-11	[The MBTW Group]	play	Link
2024-04-11	[Wencor.com]	cloak	Link
2024-04-11	[Theharriscenter.org]	cloak	Link
2024-04-11	[Community Alliance]	incransom	Link
2024-04-11	[Henningson & Snoxell, Ltd.]	incransom	Link
2024-04-11	[Optima Manufacturing]	hunters	Link
2024-04-08	[wexer.com]	darkvault	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-11	[Missouri Electric Cooperatives]	akira	Link
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
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 &amp;amp; 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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-04-05	[Doctorim]	malekteam	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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 &amp; 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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-04-01	[besttrans.com]	cactus	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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.