Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240424

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

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

—

Palo-Alto-Firewalls: Mehr Angriffe und Proofs-of-Concept aufgetaucht
Für die root-Zugriffslücke in Firewalls von Palo Alto Networks sind Proof-of-Concept-Exploits aufgetaucht. Angriffe nehmen zu.
- Link

—

Oracle: Critical Patch Update bringt 441 Sicherheitskorrekturen
Im April liefert Oracle zum Critical Patch Update (CPU) sehr viele Sicherheitsaktualisierungen aus – 441 an der Zahl.
- Link

—

Nur NIST P-521 betroffen: PuTTY-Lücke kompromittiert private SSH-Schlüssel

Bereits seit sieben Jahren schlummert die Lücke im freien Terminalclient PuTTY. Angreifer müssen jedoch einige Hürden nehmen, um SSH-Schlüssel zu klauen.

- Link

—

Kritische Lücken in Ivanti Avalanche MDM gefährden Mobilgeräte in Firmen

Ivantis Mobile-Device-Management-Lösung Avalanche ist verwundbar. Eine abgesicherte Version steht zum Download bereit.

- Link

—

Webbrowser: Sicherheitsupdates für Chrome und Firefox

Sowohl Google als auch die Mozilla-Stiftung haben Aktualisierungen ihrer Webbrowser Chrome und Firefox herausgegeben. Sie schließen viele Sicherheitslücken.

- 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	0.987590000	Link
CVE-2023-6553	0.916210000	0.988620000	Link
CVE-2023-5360	0.967230000	0.996470000	Link
CVE-2023-4966	0.968690000	0.996910000	Link
CVE-2023-48795	0.935220000	0.990650000	Link
CVE-2023-47246	0.941130000	0.991310000	Link
CVE-2023-46805	0.965580000	0.996010000	Link
CVE-2023-46747	0.971350000	0.997900000	Link
CVE-2023-46604	0.972480000	0.998380000	Link
CVE-2023-43177	0.964020000	0.995490000	Link
CVE-2023-42793	0.970710000	0.997600000	Link
CVE-2023-39143	0.938760000	0.991040000	Link
CVE-2023-38646	0.913020000	0.988370000	Link
CVE-2023-38203	0.972020000	0.998150000	Link
CVE-2023-38035	0.973610000	0.998940000	Link
CVE-2023-36845	0.966640000	0.996270000	Link
CVE-2023-3519	0.911860000	0.988320000	Link
CVE-2023-35082	0.947410000	0.992330000	Link
CVE-2023-35078	0.965840000	0.996050000	Link
CVE-2023-34993	0.956820000	0.993910000	Link
CVE-2023-34960	0.938540000	0.991020000	Link
CVE-2023-34634	0.918830000	0.988860000	Link
CVE-2023-34362	0.955450000	0.993670000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34039	0.919380000	0.988910000	Link
CVE-2023-3368	0.918440000	0.988850000	Link
CVE-2023-33246	0.973120000	0.998660000	Link
CVE-2023-32315	0.973670000	0.998970000	Link
CVE-2023-32235	0.911650000	0.988280000	Link
CVE-2023-30625	0.945200000	0.992060000	Link
CVE-2023-30013	0.960350000	0.994570000	Link
CVE-2023-29300	0.970480000	0.997470000	Link
CVE-2023-29298	0.936290000	0.990770000	Link
CVE-2023-28771	0.921620000	0.989120000	Link
CVE-2023-28432	0.940320000	0.991220000	Link
CVE-2023-28121	0.945870000	0.992140000	Link
CVE-2023-27524	0.970780000	0.997620000	Link
CVE-2023-27372	0.973490000	0.998900000	Link
CVE-2023-27350	0.972040000	0.998150000	Link
CVE-2023-26469	0.938630000	0.991030000	Link
CVE-2023-26360	0.963530000	0.995330000	Link
CVE-2023-26035	0.969280000	0.997070000	Link
CVE-2023-25717	0.957880000	0.994100000	Link
CVE-2023-25194	0.969270000	0.997070000	Link
CVE-2023-2479	0.963600000	0.995360000	Link
CVE-2023-24489	0.974290000	0.999380000	Link
CVE-2023-23752	0.952140000	0.993080000	Link
CVE-2023-23397	0.926450000	0.989760000	Link
CVE-2023-23333	0.963260000	0.995250000	Link
CVE-2023-22527	0.965680000	0.996040000	Link
CVE-2023-22518	0.966340000	0.996200000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-22515	0.971960000	0.998120000	Link
CVE-2023-21839	0.958250000	0.994170000	Link
CVE-2023-21554	0.959160000	0.994320000	Link
CVE-2023-20887	0.962160000	0.994980000	Link
CVE-2023-20198	0.900800000	0.987540000	Link
CVE-2023-1671	0.967280000	0.996500000	Link
CVE-2023-0669	0.969750000	0.997210000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 23 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

—

Tue, 23 Apr 2024

[UPDATE] [hoch] FreeRDP: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein Angreifer kann mehrere Schwachstellen in FreeRDP ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Tue, 23 Apr 2024

[UPDATE] [hoch] Grub2: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein Angreifer kann mehrere Schwachstellen in Oracle Linux ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Tue, 23 Apr 2024

[UPDATE] [hoch] Samba: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Samba ausnutzen, um

Sicherheitsvorkehrungen zu umgehen, Informationen offenzulegen, einen Denial of Service Zustand zu verursachen oder seine Rechte zu erweitern.

- Link

—

Tue, 23 Apr 2024

[UPDATE] [hoch] Nextcloud: Mehrere Schwachstellen

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Nextcloud Server und verschiedenen Apps ausnutzen, um Benutzerrechte zu erlangen, um den Benutzer zu täuschen und um Sicherheitsmechanismen zu umgehen.

- Link

—

Tue, 23 Apr 2024

[UPDATE] [hoch] Linux “Shim”: Schwachstelle ermöglicht Übernahme der Kontrolle

Ein anonymer Angreifer aus dem angrenzenden Netzwerk kann eine Schwachstelle in der “Shim” Komponente von Linux-Systemen ausnutzen, um die Kontrolle über ein betroffenes System zu übernehmen.

- Link

—

Tue, 23 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

—

Tue, 23 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

—

Tue, 23 Apr 2024

[UPDATE] [hoch] Oracle Communications Applications: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Communications Applications ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- Link

—

Tue, 23 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

—

Tue, 23 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

—

Mon, 22 Apr 2024

[NEU] [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

—

Mon, 22 Apr 2024

[NEU] [hoch] PyTorch: Schwachstelle ermöglicht Denial of Service und Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PyTorch ausnutzen, um Informationen offenzulegen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Mon, 22 Apr 2024

[NEU] [hoch] ffmpeg: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in ffmpeg ausnutzen, um beliebigen Code auszuführen oder einen ‘Denial of Service’-Zustand zu verursachen.

- Link

—

Mon, 22 Apr 2024

[NEU] [hoch] Microsoft GitHub Enterprise: Mehrere Schwachstellen

Ein entfernter authentifizierter Angreifer kann mehrere Schwachstellen in Microsoft GitHub Enterprise ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen oder Dateien zu manipulieren.

- Link

—

Mon, 22 Apr 2024

[NEU] [hoch] ffmpeg: Mehrere Schwachstellen ermöglichen Denial of Service

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

- Link

—

Mon, 22 Apr 2024

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

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

- Link

—

Mon, 22 Apr 2024

[UPDATE] [hoch] VMware Tanzu Spring Framework: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in VMware Tanzu Spring Framework ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Mon, 22 Apr 2024

[UPDATE] [hoch] Red Hat Enterprise Linux (python-reportlab): Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux in der Komponente “python-reportlab” ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 22 Apr 2024

[UPDATE] [hoch] Red Hat Satellite: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat Satellite ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
4/23/2024	[RHEL 8 : OpenShift Container Platform 4.9.56 (RHSA-2023:0777)]	critical
4/23/2024	[RHEL 8 : Red Hat OpenStack Platform 16.2 (etcd) (RHSA-2023:3445)]	critical
4/23/2024	[RHEL 8 : Red Hat Product OCP Tools 4.14 Openshift Jenkins (RHSA-2023:7288)]	critical
4/23/2024	[RHEL 8 : OpenShift Container Platform 4.9.55 (RHSA-2023:0573)]	critical
4/23/2024	[CBL Mariner 2.0 Security Update: cups (CVE-2023-34241)]	high
4/23/2024	[CBL Mariner 2.0 Security Update: cri-o (CVE-2022-1708)]	high
4/23/2024	[CBL Mariner 2.0 Security Update: cups (CVE-2023-4504)]	high
4/23/2024	[Slackware Linux 15.0 / current freerdp Vulnerability (SSA:2024-113-01)]	high
4/23/2024	[Ubuntu 22.04 LTS : Linux kernel (Low Latency) vulnerabilities (USN-6743-2)]	high
4/23/2024	[SUSE SLES15 Security Update : kernel RT (Live Patch 7 for SLE 15 SP5) (SUSE-SU-2024:1359-1)]	high
4/23/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : glibc (SUSE-SU-2024:1375-1)]	high
4/23/2024	[SUSE SLES15 Security Update : kernel RT (Live Patch 10 for SLE 15 SP5) (SUSE-SU-2024:1362-1)]	high
4/23/2024	[SUSE SLES15 Security Update : kernel RT (Live Patch 8 for SLE 15 SP5) (SUSE-SU-2024:1364-1)]	high
4/23/2024	[SUSE SLES15 Security Update : kernel (Live Patch 21 for SLE 15 SP4) (SUSE-SU-2024:1386-1)]	high
4/23/2024	[SUSE SLES12 Security Update : kernel (Live Patch 48 for SLE 12 SP5) (SUSE-SU-2024:1382-1)]	high
4/23/2024	[SUSE SLES15 Security Update : kernel (Live Patch 1 for SLE 15 SP5) (SUSE-SU-2024:1380-1)]	high

Datum	Schwachstelle	Bewertung
4/23/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : shim (SUSE-SU-2024:1368-1)]	high
4/23/2024	[Debian dsa-5673 : glibc-doc - security update]	high
4/23/2024	[SUSE SLES12 Security Update : kernel (Live Patch 51 for SLE 12 SP5) (SUSE-SU-2024:1373-1)]	high
4/23/2024	[RHEL 7 : shim (RHSA-2024:1959)]	high
4/23/2024	[RHEL 8 : go-toolset:rhel8 (RHSA-2024:1962)]	high
4/23/2024	[Fedora 39 : chromium (2024-12edb9dec8)]	high
4/23/2024	[Fedora 39 : cjson (2024-74563262c0)]	high
4/23/2024	[RHEL 8 : kpatch-patch (RHSA-2024:1961)]	high
4/23/2024	[Oracle Linux 9 : gnutls (ELSA-2024-12336)]	high
4/23/2024	[Oracle Linux 6 : kernel (ELSA-2024-1831)]	high
4/23/2024	[SUSE SLES15 Security Update : kernel RT (Live Patch 1 for SLE 15 SP5) (SUSE-SU-2024:1358-1)]	high
4/23/2024	[Ubuntu 16.04 LTS / 18.04 LTS : Percona XtraBackup vulnerability (USN-6745-1)]	high
4/23/2024	[Debian dla-3791 : thunderbird - security update]	high
4/23/2024	[RHEL 8 / 9 : OpenShift Container Platform 4.13.23 (RHSA-2023:7325)]	high
4/23/2024	[RHEL 7 / 8 : OpenShift Container Platform 4.10.67 (RHSA-2023:4898)]	high
4/23/2024	[RHEL 8 : OpenShift Container Platform 4.11.34 (RHSA-2023:1503)]	high
4/23/2024	[RHEL 8 : OpenShift Virtualization 4.14.1 RPMs (RHSA-2023:7672)]	high
4/23/2024	[RHEL 9 : Red Hat OpenStack Platform 17.1.1 (RHSA-2023:5969)]	high
4/23/2024	[RHEL 7 : thunderbird (RHSA-2024:1498)]	high
4/23/2024	[RHEL 7 : tigervnc (RHSA-2024:0006)]	high

Datum	Schwachstelle	Bewertung
4/23/2024	[AlmaLinux 9 : firefox (ALSA-2024:1908)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“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.

- 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

—

” “Thu, 18 Apr 2024

Elber ESE DVB-S/S2 Satellite Receiver 1.5.x Authentication Bypass

Elber ESE DVB-S/S2 Satellite Receiver version 1.5.x 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.

- Link

—

” “Thu, 18 Apr 2024

Elber Reble610 M/ODU XPIC IP-ASI-SDH Microwave Link Insecure Direct Object Reference

Elber Reble610 M/ODU XPIC IP-ASI-SDH Microwave Link suffers from an unauthenticated device configuration and client-side hidden functionality disclosure vulnerability.

- Link

—

” “Thu, 18 Apr 2024

Elber Reble610 M/ODU XPIC IP-ASI-SDH Microwave Link Authentication Bypass

Elber Reble610 M/ODU XPIC IP-ASI-SDH Microwave Link 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.

- Link

—

" "Thu, 18 Apr 2024

Elber Cleber/3 Broadcast Multi-Purpose Platform 1.0.0 Insecure Direct Object Reference

Elber Cleber/3 Broadcast Multi-Purpose Platform version 1.0.0 suffers from an unauthenticated device configuration and client-side hidden functionality disclosure vulnerability.

- Link

—

" "Thu, 18 Apr 2024

Elber Cleber/3 Broadcast Multi-Purpose Platform 1.0.0 Authentication Bypass

Elber Cleber/3 Broadcast Multi-Purpose Platform version 1.0.0 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.

- Link

—

" "Thu, 18 Apr 2024

Elber Signum DVB-S/S2 IRD For Radio Networks 1.999 Insecure Direct Object Reference

Elber Signum DVB-S/S2 IRD for Radio Networks version 1.999 suffers from an unauthenticated device configuration and client-side hidden functionality disclosure vulnerability.

- Link

—

" "Thu, 18 Apr 2024

Elber Signum DVB-S/S2 IRD For Radio Networks 1.999 Authentication Bypass

Elber Signum DVB-S/S2 IRD for Radio Networks version 1.999 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.

- Link

—
”

4.2 0-Days der letzten 5 Tage

“Tue, 23 Apr 2024
ZDI-24-396: Microsoft Azure ODSP nikisos Uncontrolled Search Path Element Remote Code Execution Vulnerability
- Link
—
” “Tue, 23 Apr 2024
ZDI-24-395: Ivanti Avalanche WLInfoRailService DELKEY Directory Traversal Arbitrary File Deletion Vulnerability
- Link
—
” “Tue, 23 Apr 2024
ZDI-24-394: Ivanti Avalanche WLAvalancheService Null Pointer Dereference Denial-of-Service Vulnerability
- Link
—
” “Tue, 23 Apr 2024
ZDI-24-393: Ivanti Avalanche WLAvalancheService Directory Traversal Arbitrary File Deletion Vulnerability
- Link
—
” “Tue, 23 Apr 2024
ZDI-24-392: Ivanti Avalanche WLAvalancheService Directory Traversal Remote Code Execution Vulnerability
- Link
—
” “Tue, 23 Apr 2024
ZDI-24-391: Ivanti Avalanche WLAvalancheService Use-After-Free Remote Code Execution Vulnerability
- Link
—
” “Tue, 23 Apr 2024
ZDI-24-390: Ivanti Avalanche WLAvalancheService Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-389: Ivanti Avalanche WLAvalancheService Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-388: Ivanti Avalanche WLAvalancheService Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-387: Ivanti Avalanche WLAvalancheService Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-386: Ivanti Avalanche WLInfoRailService Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-385: Ivanti Avalanche doInTransaction Time-Of-Check Time-Of-Use Remote Code Execution Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-384: Ivanti Avalanche extractZipEntry Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-383: Ivanti Avalanche InstallPackageThread Time-Of-Check Time-Of-Use Remote Code Execution Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-382: Ivanti Avalanche getAdhocFilePath Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-381: Ivanti Avalanche WLAvalancheService Null Pointer Dereference Denial-of-Service Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-380: Ivanti Avalanche copyFile Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-379: Ivanti Avalanche getMasterAdhocCollectionsPath Unrestricted File Upload Remote Code Execution Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-378: Ivanti Avalanche WLAvalancheService Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-377: Ivanti Avalanche WLAvalancheService Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-376: Ivanti Avalanche WLInfoRailService Integer Overflow Information Disclosure Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-375: Ivanti Avalanche WLAvalancheService Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-374: Ivanti Avalanche WLAvalancheService Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-373: Ivanti Avalanche WLAvalancheService Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-372: Ivanti Avalanche WLAvalancheService Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-371: Ivanti Avalanche WLAvalancheService Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 23 Apr 2024

ZDI-24-370: Ivanti Avalanche WLInfoRailService Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Apr 2024

ZDI-24-369: Google cAdvisor REST API Improper Access Control Information Disclosure Vulnerability

- Link

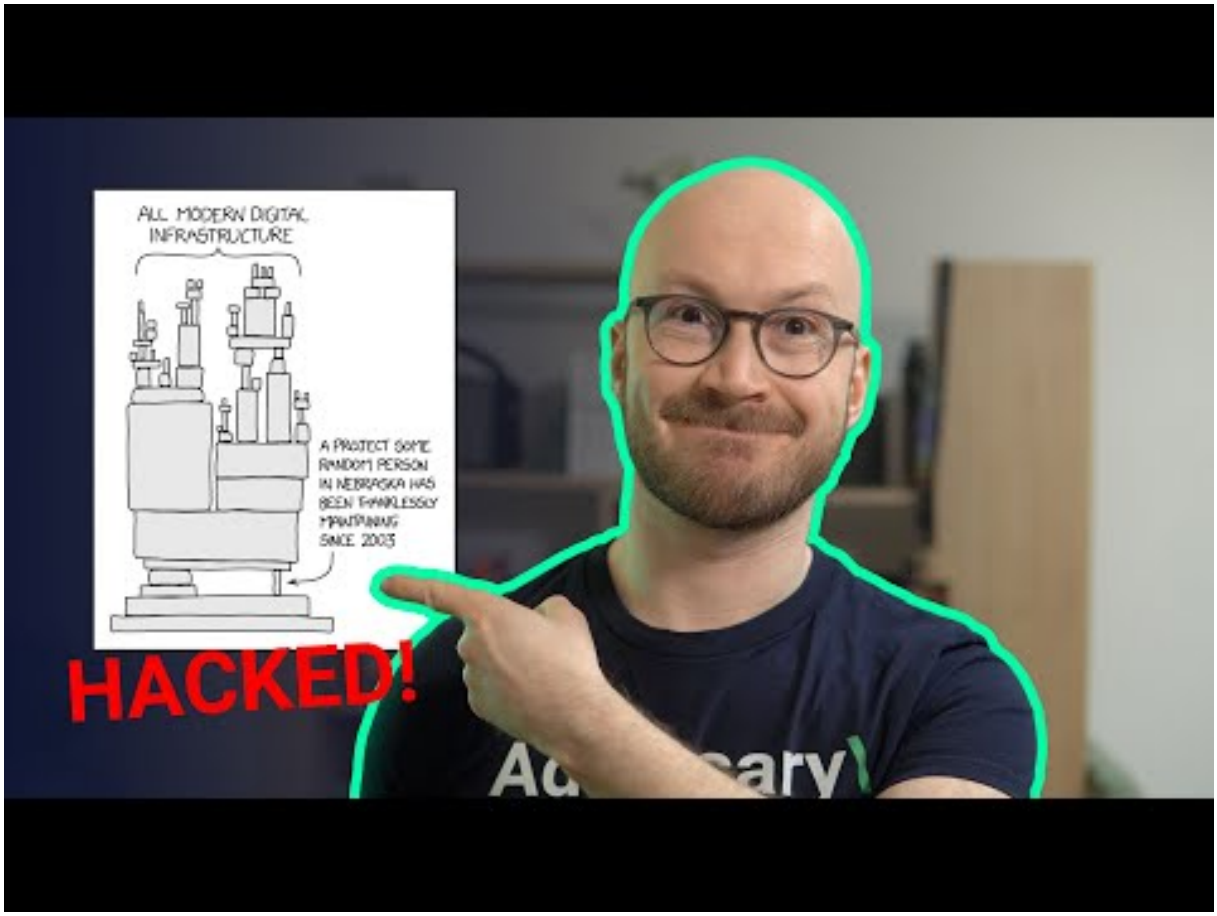
—

”

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
2024-04-23	Skanlog	[SWE]	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
2024-04-14	Plus Servicios	[CHL]	Link
2024-04-14	Frontier Communications	[USA]	Link
2024-04-14	Le ministère de la Santé de la République Dominicaine.	[DOM]	Link
2024-04-13	Tyler Technologies	[USA]	Link

Datum	Opfer	Land	Information
2024-04-11	Taiwan United Renewable Energy Corporation (URECO)	[TWN]	Link
2024-04-11	Swinomish Casino and Lodge	[USA]	Link
2024-04-11	Iddink Learning Materials	[NLD]	Link
2024-04-10	Ville de Saint-Nazaire et son agglomération	[FRA]	Link
2024-04-10	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
2024-04-23	[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]	eraleig	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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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.com]	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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-04-09	[Hudson Supplies]	blacksuit	Link
2024-04-09	[Homeocan]	blacksuit	Link
2024-04-09	[Macuz]	ciphbit	Link

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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-04-04	[Remitano - Cryptocurrency Exchange]	incransom	Link
2024-04-04	[mcalvain.com]	cactus	Link
2024-04-03	[Precision Pulley & Idler]	blacksuit	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-04-02	[regencyfurniture.com]	cactus	Link
2024-04-02	[KICO GROUP]	raworld	Link
2024-04-02	[GRUPOCREATIVO HERRERA]	qilin	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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.