Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240423

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	0.987560000	Link
CVE-2023-6553	0.916210000	0.988600000	Link
CVE-2023-5360	0.967230000	0.996470000	Link
CVE-2023-4966	0.968690000	0.996900000	Link
CVE-2023-48795	0.935220000	0.990640000	Link
CVE-2023-47246	0.941130000	0.991290000	Link
CVE-2023-46805	0.965580000	0.996010000	Link
CVE-2023-46747	0.971350000	0.997900000	Link
CVE-2023-46604	0.972480000	0.998390000	Link
CVE-2023-43177	0.964020000	0.995490000	Link
CVE-2023-42793	0.970710000	0.997590000	Link
CVE-2023-39143	0.938760000	0.991020000	Link
CVE-2023-38646	0.928720000	0.989980000	Link
CVE-2023-38203	0.972020000	0.998140000	Link
CVE-2023-38035	0.973610000	0.998940000	Link
CVE-2023-36845	0.966640000	0.996270000	Link
CVE-2023-3519	0.911860000	0.988300000	Link
CVE-2023-35082	0.947410000	0.992320000	Link
CVE-2023-35078	0.965840000	0.996050000	Link
CVE-2023-34993	0.956820000	0.993900000	Link
CVE-2023-34960	0.938540000	0.991000000	Link
CVE-2023-34634	0.918830000	0.988840000	Link
CVE-2023-34362	0.955450000	0.993660000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34039	0.919380000	0.988890000	Link
CVE-2023-3368	0.918440000	0.988820000	Link
CVE-2023-33246	0.972820000	0.998530000	Link
CVE-2023-32315	0.973670000	0.998970000	Link
CVE-2023-32235	0.911650000	0.988270000	Link
CVE-2023-30625	0.945200000	0.992030000	Link
CVE-2023-30013	0.960350000	0.994570000	Link
CVE-2023-29300	0.970480000	0.997480000	Link
CVE-2023-29298	0.936290000	0.990760000	Link
CVE-2023-28771	0.921620000	0.989100000	Link
CVE-2023-28432	0.943220000	0.991630000	Link
CVE-2023-28121	0.945870000	0.992110000	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	0.991010000	Link
CVE-2023-26360	0.963530000	0.995330000	Link
CVE-2023-26035	0.969280000	0.997070000	Link
CVE-2023-25717	0.957880000	0.994090000	Link
CVE-2023-25194	0.969270000	0.997070000	Link
CVE-2023-2479	0.963600000	0.995360000	Link
CVE-2023-24489	0.973920000	0.999100000	Link
CVE-2023-23752	0.952140000	0.993070000	Link
CVE-2023-23397	0.926450000	0.989740000	Link
CVE-2023-23333	0.963260000	0.995250000	Link
CVE-2023-22527	0.965680000	0.996030000	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	0.958450000	0.994200000	Link
CVE-2023-21554	0.959160000	0.994310000	Link
CVE-2023-20887	0.962160000	0.994980000	Link
CVE-2023-20198	0.900800000	0.987510000	Link
CVE-2023-1671	0.967910000	0.996700000	Link
CVE-2023-0669	0.969750000	0.997210000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 22 Apr 2024

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

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

- Link

—

Mon, 22 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

—

Mon, 22 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, 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

—

Mon, 22 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

—

Mon, 22 Apr 2024

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

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

- Link

—

Mon, 22 Apr 2024

[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge

ausnutzen, um beliebigen Programmcode auszuführen und weitere, nicht spezifizierte Auswirkungen zu verursachen.

- Link

—

Fri, 19 Apr 2024

[UPDATE] [hoch] VMware Tanzu Spring Security: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in VMware Tanzu Spring Security ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Fri, 19 Apr 2024

[UPDATE] [kritisch] Apache ActiveMQ: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Fri, 19 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

—

Fri, 19 Apr 2024

[UPDATE] [hoch] pgAdmin: Schwachstelle ermöglicht Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in pgAdmin ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 18 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

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
4/22/2024	[Siemens SINEC NMS TFTP File Upload (CVE-2024-23811)]	critical
4/21/2024	[RHEL 5 : pki (RHSA-2010:0838)]	critical
4/21/2024	[RHEL 5 : httpd and httpd22 (RHSA-2010:0011)]	critical
4/21/2024	[RHEL 5 : redhat-ds-base (RHSA-2008:0269)]	critical
4/21/2024	[RHEL 6 : openstack-keystone (RHSA-2013:0994)]	critical
4/21/2024	[RHEL 6 / 7 : php54 (RHSA-2015:1066)]	critical
4/21/2024	[Mitsubishi MELSEC-Q/L Series Integer Overflow or Wraparound (CVE-2024-0803)]	critical
4/21/2024	[Mitsubishi MELSEC-Q/L Series Integer Overflow or Wraparound (CVE-2024-1916)]	critical
4/21/2024	[Mitsubishi MELSEC-Q/L Series Incorrect Pointer Scaling (CVE-2024-1915)]	critical
4/21/2024	[Mitsubishi MELSEC-Q/L Series Incorrect Pointer Scaling (CVE-2024-0802)]	critical
4/21/2024	[Mitsubishi MELSEC-Q/L Series Integer Overflow or Wraparound (CVE-2024-1917)]	critical
4/22/2024	[Adobe ColdFusion Arbitrary File Read]	high
4/22/2024	[RHEL 9 : nodejs:18 (RHSA-2024:1932)]	high
4/22/2024	[RHEL 7 : CloudForms 4.7.5 (RHSA-2019:1429)]	high
4/22/2024	[RHEL 6 / 7 : rh-python35-python-jinja2 (RHSA-2019:1237)]	high
4/22/2024	[RHEL 8 : Red Hat OpenStack Platform 17.1 (openstack-tripleo-heat-templates and python-yaql) (RHSA-2024:1930)]	high
4/22/2024	[FreeBSD : chromium – multiple security fixes (9bed230f-ffc8-11ee-8e76-a8a1599412c6)]	high
4/22/2024	[Siemens SIMATIC S7-1500 Use After Free (CVE-2023-6932)]	high

Datum	Schwachstelle	Bewertung
4/22/2024	[Siemens SIMATIC S7-1500 Improper Input Validation (CVE-2023-45898)]	high
4/22/2024	[Siemens SIMATIC S7-1500 Out-of-bounds Write (CVE-2023-6931)]	high
4/22/2024	[Siemens SIMATIC S7-1500 Use After Free (CVE-2023-6817)]	high
4/21/2024	[RHEL 5 / 6 : httpd and httpd22 (RHSA-2011:1329)]	high
4/21/2024	[Fedora 38 : firefox (2024-966e16bfa3)]	high
4/21/2024	[Fedora 38 : mod_http2 (2024-1f11550e31)]	high
4/21/2024	[Fedora 38 : chromium (2024-5d8f4f86b0)]	high
4/21/2024	[Fedora 39 : mod_http2 (2024-528301bac2)]	high
4/21/2024	[RHEL 6 : openstack-keystone (RHSA-2013:1285)]	high
4/21/2024	[RHEL 6 : openstack-cinder (RHSA-2013:1198)]	high
4/20/2024	[RHEL 9 : shim update (Important) (RHSA-2024:1903)]	high
4/20/2024	[RHEL 8 / 9 : OpenShift Container Platform 4.13.40 (RHSA-2024:1763)]	high
4/20/2024	[FreeBSD : clamav – Possible crash in the HTML file parser that could cause a denial-of-service (DoS) condition (ecafc4af-fe8a-11ee-890c-08002784c58d)]	high
4/20/2024	[Debian dsa-5668 : chromium - security update]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“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

—

” “Thu, 18 Apr 2024

Relate Cross Site Scripting

Relate learning and teaching system versions prior to 2024.1 suffer from a persistent cross site

scripting vulnerability.

- Link

—

” “Wed, 17 Apr 2024

Palo Alto OS Command Injection

Palo Alto OS was recently hit by a command injection zero day attack. These are exploitation details related to the zero day.

- Link

—

” “Wed, 17 Apr 2024

Palo Alto OS Command Injection Proof Of Concept

This is a scanning script to validate vulnerable Palo Alto OS systems for the recent zero day command injection vulnerability.

- Link

—

” “Wed, 17 Apr 2024

pgAdmin 8.3 Remote Code Execution

pgAdmin versions 8.3 and below have a path traversal vulnerability within their session management logic that can allow a pickled file to be loaded from an arbitrary location. This can be used to load a malicious, serialized Python object to execute code within the context of the target application. This exploit supports two techniques by which the payload can be loaded, depending on whether or not credentials are specified. If valid credentials are provided, Metasploit will login to pgAdmin and upload a payload object using pgAdmin’s file management plugin. Once uploaded, this payload is executed via the path traversal before being deleted using the file management plugin. This technique works for both Linux and Windows targets. If no credentials are provided, Metasploit will start an SMB server and attempt to trigger loading the payload via a UNC path. This technique only works for Windows targets. For Windows 10 v1709 (Redstone 3) and later, it also requires that insecure outbound guest access be enabled. Tested on pgAdmin 8.3 on Linux, 7.7 on Linux, 7.0 on Linux, and 8.3 on Windows. The file management plugin underwent changes in the 6.x versions and therefore, pgAdmin versions below 7.0 cannot utilize the authenticated technique whereby a payload is uploaded.

- Link

—

” “Tue, 16 Apr 2024

Centreon 23.10-1.el8 SQL Injection

Centreon version 23.10-1.el8 suffers from a remote authenticated SQL injection vulnerability.

- Link

—

” “Tue, 16 Apr 2024

Backdoor.Win32.Dumador.c MVID-2024-0679 Buffer Overflow

Backdoor.Win32.Dumador.c malware suffers from a buffer overflow vulnerability.

- Link

—

” “Mon, 15 Apr 2024

Amazon AWS Glue Database Password Disclosure

The password of database connections in AWS Glue is loaded into the website when a connection’s edit page is requested. Principals with appropriate permissions can read the password. This behavior also increases the risk that database passwords will be intercepted by an attacker during transmission in the server response. Many types of vulnerabilities, such as broken access controls, cross site scripting and weaknesses in session handling, could enable an attacker to leverage this behavior to retrieve the passwords.

- Link

—

” “Mon, 15 Apr 2024

CrushFTP Remote Code Execution

This Metasploit exploit module leverages an improperly controlled modification of dynamically-determined object attributes vulnerability (CVE-2023-43177) to achieve unauthenticated remote code execution. This affects CrushFTP versions prior to 10.5.1. It is possible to set some user’s session properties by sending an HTTP request with specially crafted Header key-value pairs. This enables an unauthenticated attacker to access files anywhere on the server file system and steal the session cookies of valid authenticated users. The attack consists in hijacking a user’s session and escalates privileges to obtain full control of the target. Remote code execution is obtained by abusing the dynamic SQL driver loading and configuration testing feature.

- Link

—

” “Mon, 15 Apr 2024

GLPI 10.x.x Remote Command Execution

GLPI versions 10.x.x suffers from a remote command execution vulnerability via the shell commands plugin.

- Link

—

” “Mon, 15 Apr 2024

WordPress WP Video Playlist 1.1.1 Cross Site Scripting

WordPress WP Video Playlist plugin version 1.1.1 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Mon, 15 Apr 2024

BMC Compuware iStrobe Web 20.13 Shell Upload

BMC Compuware iStrobe Web version 20.13 suffers from a remote shell upload vulnerability.

- Link

—

” “Mon, 15 Apr 2024

Kruxton 1.0 SQL Injection

Kruxton version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 15 Apr 2024

Kruxton 1.0 Shell Upload

Kruxton version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Mon, 15 Apr 2024

WBCE 1.6.0 SQL Injection

WBCE version 1.6.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 15 Apr 2024

AMPLE BILLS 0.1 SQL injection

AMPLE BILLS version 0.1 suffers from a remote SQL injection vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Mon, 22 Apr 2024

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

- Link

—

” “Fri, 19 Apr 2024

ZDI-24-368: GStreamer AV1 Video Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

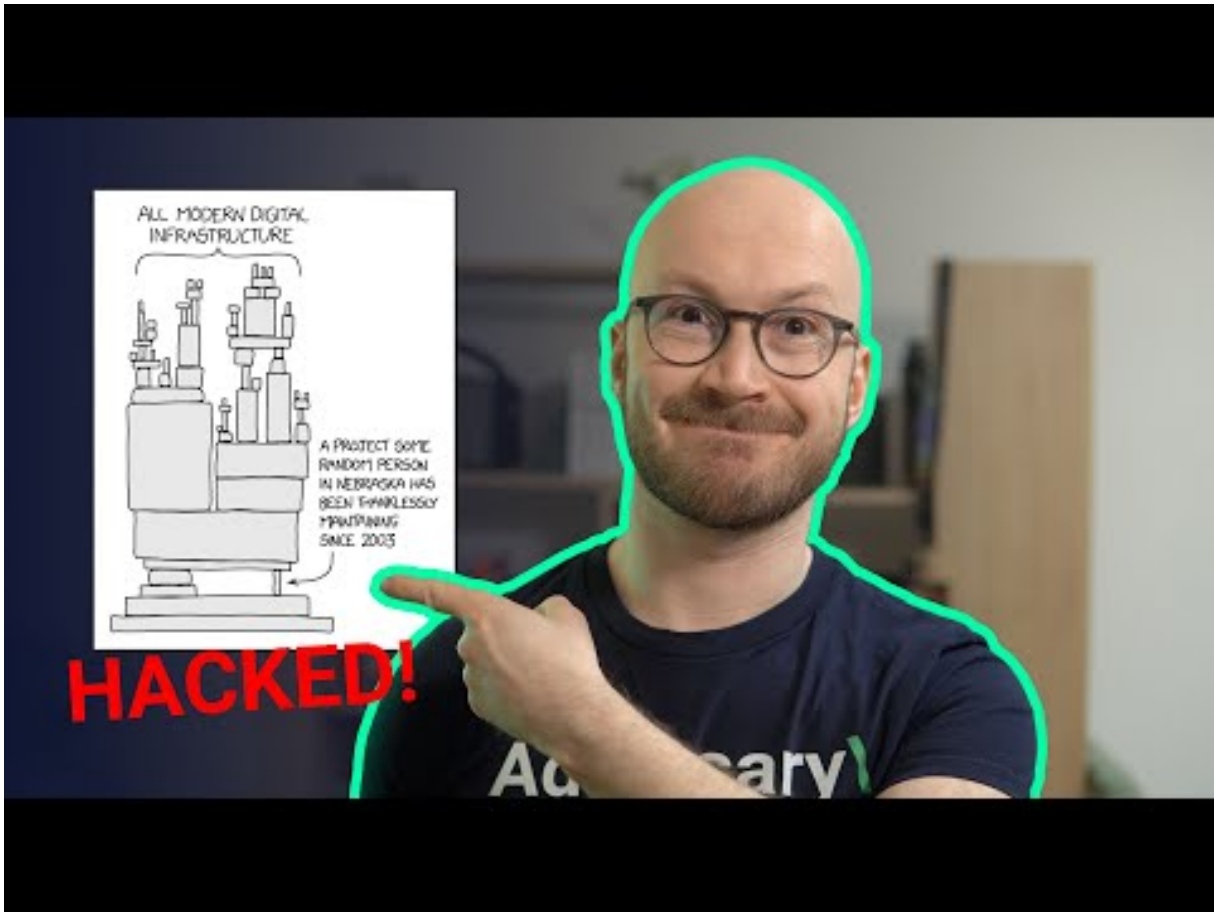
—

”

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
2024-04-22	Ville d'Albi	[FRA]	Link
2024-04-20	▯▯▯▯ (Union Hospital)	[HKG]	Link
2024-04-19	Swisspro	[CHE]	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
2024-04-16	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
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

Datum	Opfer	Land	Information
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
2024-04-22	[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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.