Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240628

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

APT-Angriff auf Fernwartungssoftware? Sicherheitsvorfall bei TeamViewer

Noch ist über das Ausmaß des Angriffs gegen die Fernwartungssoftware nicht viel bekannt - erste Hinweise auf die Urheber deuten auf Profis hin.

- Link

—

Bitte patchen! Security-Update behebt kritische Schwachstelle in GitLab

Eine Reihe von Schwachstellen ermöglichen es in GitLab, CI-Pipelines als anderer User zu starten oder Cross-Site-Scripting über Commit Notes einzuschleusen.

- Link

—

Google Quickshare: Sicherheitslücke ermöglicht ungefragtes Senden von Dateien

Googles Quickshare, auch als Nearby Share bekannt, kann Angreifern ungefragt Daten an Windows-Rechner schicken lassen.

- Link

—

JavaScript-Service Polyfill.io: 100.000 Sites binden Schadcode über CDN ein

Mehrere Sicherheitsforscher melden eine aktive Bedrohung durch das Content Delivery Network von Polyfill.io. Google sperrt Werbung von betroffenen Ads-Seiten.

- Link

—

Jetzt patchen! Progress-MOVEit-Sicherheitslücken werden bereits angegriffen

Progress hat zwei kritische Lücken in MOVEit Gateway und Transfer gestopft. Eine davon missbrauchen Cyberkriminelle bereits.

- Link

—

Wordpress: Fünf Plug-ins mit Malware unterwandert

In fünf Wordpress-Plug-ins haben IT-Sicherheitsforscher dieselbe eingeschleuste Malware entdeckt. Nur für eines gibt es ein Update.

- Link

—

Juniper: 225 Sicherheitslücken in Secure Analytics

Juniper Networks hat eine Aktualisierung für Secure Analytics herausgegeben. Sie stopft 225 Sicherheitslecks, einige davon gelten als kritisch.

- Link

—

PCs mit Intel-Prozessoren: UEFI-Sicherheitslücke lässt Schadcode passieren

Aufgrund eines Fehlers in der UEFI-Firmware von Phoenix können Angreifer Computer attackieren. Davon sind unter anderem Lenovo-Geräte mit Intel-CPU betroffen.

- Link

—

Jetzt patchen! Angreifer attackieren Dateiübertragungsserver SolarWinds Serv-U

Im Zuge von Attacken auf SolarWinds Serv-U verschaffen sich Angreifer Zugang auf eigentlich abgeschottete Dateien.

- Link

—

Sicherheitslücken: Attacken auf Atlassian Confluence & Co. möglich

Sicherheitslücken bedrohen mehrere Anwendungen von Atlassian. Angreifer können Abstürze auslösen oder unbefugt Daten einsehen.

- 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-2023-7028	0.960230000	0.994930000	Link
CVE-2023-6895	0.920390000	0.989540000	Link
CVE-2023-6553	0.928510000	0.990410000	Link
CVE-2023-5360	0.911260000	0.988810000	Link
CVE-2023-4966	0.971290000	0.998030000	Link
CVE-2023-49103	0.941230000	0.991860000	Link
CVE-2023-48795	0.962520000	0.995390000	Link
CVE-2023-47246	0.943030000	0.992080000	Link
CVE-2023-46805	0.958670000	0.994640000	Link
CVE-2023-46747	0.972100000	0.998340000	Link
CVE-2023-46604	0.931360000	0.990740000	Link
CVE-2023-4542	0.924200000	0.989970000	Link
CVE-2023-43208	0.956050000	0.994230000	Link
CVE-2023-43177	0.959300000	0.994780000	Link
CVE-2023-42793	0.970430000	0.997650000	Link
CVE-2023-41265	0.920320000	0.989520000	Link
CVE-2023-39143	0.944760000	0.992360000	Link
CVE-2023-38205	0.945440000	0.992470000	Link
CVE-2023-38203	0.968820000	0.997180000	Link
CVE-2023-38146	0.905210000	0.988400000	Link
CVE-2023-38035	0.974620000	0.999590000	Link
CVE-2023-36845	0.964620000	0.995910000	Link
CVE-2023-3519	0.912170000	0.988880000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-35082	0.967870000	0.996910000	Link
CVE-2023-35078	0.968330000	0.997060000	Link
CVE-2023-34993	0.971260000	0.998030000	Link
CVE-2023-34960	0.922260000	0.989710000	Link
CVE-2023-34634	0.920590000	0.989550000	Link
CVE-2023-34468	0.906650000	0.988500000	Link
CVE-2023-34362	0.957100000	0.994400000	Link
CVE-2023-34039	0.945410000	0.992460000	Link
CVE-2023-3368	0.933870000	0.991030000	Link
CVE-2023-33246	0.973320000	0.998880000	Link
CVE-2023-32315	0.973600000	0.999040000	Link
CVE-2023-30625	0.938290000	0.991490000	Link
CVE-2023-30013	0.962250000	0.995310000	Link
CVE-2023-29300	0.969840000	0.997470000	Link
CVE-2023-29298	0.943950000	0.992200000	Link
CVE-2023-28771	0.918640000	0.989400000	Link
CVE-2023-28121	0.923740000	0.989870000	Link
CVE-2023-27524	0.970400000	0.997640000	Link
CVE-2023-27372	0.973630000	0.999050000	Link
CVE-2023-27350	0.971140000	0.997960000	Link
CVE-2023-26469	0.932230000	0.990850000	Link
CVE-2023-26360	0.947780000	0.992870000	Link
CVE-2023-26035	0.965720000	0.996250000	Link
CVE-2023-25717	0.956860000	0.994350000	Link
CVE-2023-25194	0.970160000	0.997550000	Link
CVE-2023-2479	0.963760000	0.995720000	Link
CVE-2023-24489	0.973550000	0.999010000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23752	0.948880000	0.993050000	Link
CVE-2023-23397	0.915470000	0.989150000	Link
CVE-2023-23333	0.963260000	0.995590000	Link
CVE-2023-22527	0.972640000	0.998560000	Link
CVE-2023-22518	0.965950000	0.996300000	Link
CVE-2023-22515	0.973330000	0.998900000	Link
CVE-2023-21839	0.955020000	0.994040000	Link
CVE-2023-21554	0.950840000	0.993330000	Link
CVE-2023-20887	0.966680000	0.996500000	Link
CVE-2023-1671	0.964510000	0.995880000	Link
CVE-2023-0669	0.968870000	0.997190000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Thu, 27 Jun 2024

[NEU] [hoch] GitLab: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren, seine Privilegien zu erweitern oder einen Cross-Site-Scripting (XSS)-Angriff durchzuführen.

- Link

—

Thu, 27 Jun 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in wpa_supplicant und hostapd ausnutzen, um Dateien zu manipulieren.

- Link

—

Thu, 27 Jun 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in OpenSSL ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.

- Link

—

Thu, 27 Jun 2024

[UPDATE] [hoch] Intel BIOS: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein lokaler Angreifer kann mehrere Schwachstellen im Intel BIOS ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Thu, 27 Jun 2024

[UPDATE] [hoch] Intel Chipset: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in der Intel Chipset Firmware ausnutzen, um seine Privilegien zu erhöhen, einen Denial of Service Zustand herbeizuführen oder Dateien zu manipulieren.

- Link

—

Thu, 27 Jun 2024

[UPDATE] [hoch] Intel BIOS: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein lokaler Angreifer kann mehrere Schwachstellen im BIOS für verschiedene Intel Prozessoren ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Thu, 27 Jun 2024

[UPDATE] [hoch] Dell PowerEdge: Schwachstelle ermöglicht Erlangen von Administratorrechten

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Dell PowerEdge ausnutzen, um Administratorrechte zu erlangen.

- Link

—

Thu, 27 Jun 2024

[UPDATE] [hoch] Sophos Unified Threat Management (UTM) Software: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Sophos Unified Threat Management (UTM) Software ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Thu, 27 Jun 2024

[UPDATE] [hoch] Intel Firmware: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Intel Firmware ausnutzen, um seine Privilegien zu erhöhen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Thu, 27 Jun 2024

[UPDATE] [kritisch] Microsoft Windows: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Windows ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, beliebigen Programmcode auszuführen, seine Privilegien zu erweitern, einen Denial of Service Zustand herbeizuführen, Dateien zu manipulieren, Sicherheitsvorkehrungen zu umgehen oder Infor mationen offenzulegen.
- Link

—

Thu, 27 Jun 2024

[UPDATE] [hoch] Ruby: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Ruby ausnutzen, um Informationen offenzulegen oder Code auszuführen.
- Link

—

Thu, 27 Jun 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

—

Thu, 27 Jun 2024

[UPDATE] [hoch] GNU libc: Schwachstelle ermöglicht Codeausführung

Ein Angreifer kann eine Schwachstelle in GNU libc ausnutzen, um einen Denial-of-Service-Zustand zu verursachen, Code auszuführen oder seine Privilegien zu erweitern.
- Link

—

Thu, 27 Jun 2024

[UPDATE] [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

—

Thu, 27 Jun 2024

[UPDATE] [hoch] ffmpeg: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Thu, 27 Jun 2024

[UPDATE] [hoch] Check Point Security Gateway: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Check Point Security Gateway ausnutzen, um Informationen offenzulegen.

- Link

—

Thu, 27 Jun 2024

[UPDATE] [hoch] Red Hat OpenShift: Mehrere Schwachstellen ermöglichen Offenlegung von Informationen und Dateimanipulation

Ein lokaler Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um Informationen offenzulegen und Dateien zu manipulieren.

- Link

—

Wed, 26 Jun 2024

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in git ausnutzen, um beliebigen Programmcode mit Benutzerrechten auszuführen oder um Daten zu manipulieren.

- Link

—

Wed, 26 Jun 2024

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in git ausnutzen, um Sicherheitsvorkehrungen zu umgehen, Daten zu manipulieren und seine Privilegien zu erweitern.

- Link

—

Wed, 26 Jun 2024

[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
6/27/2024	[GitLab 15.8 < 16.11.5 / 17.0 < 17.0.3 / 17.1 < 17.1.1 (CVE-2024-5655)]	critical
6/27/2024	[FreeBSD : Gitlab – Vulnerabilities (589de937-343f-11ef-8a7b-001b217b3468)]	critical
6/27/2024	[Fortra FileCatalyst Workflow SQLi (CVE-2024-5276) (Version Check)]	critical
6/27/2024	[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : libcdio vulnerability (USN-6855-1)]	critical
6/27/2024	[Ubuntu 22.04 LTS : OpenSSL vulnerability (USN-6854-1)]	high
6/27/2024	[GitLab 16.9 < 16.11.5 / 17.0 < 17.0.3 / 17.1 < 17.1.1 (CVE-2024-4901)]	high
6/27/2024	[GitLab 16.11.0 < 16.11.5 / 17.0.0 < 17.0.3 / 17.1.0 < 17.1.1 (CVE-2024-6323)]	high
6/27/2024	[Atlassian Confluence 1.0.1 < 7.19.22 / 7.20.x < 8.5.9 / 8.6.x < 8.9.1 (CONFSERVER-95840)]	high
6/27/2024	[IBM WebSphere eXtreme Scale 8.6.1.0 < 8.6.1.6 (7150929)]	high
6/27/2024	[RHEL 9 : OpenShift Container Platform 4.16.0 (RHSA-2024:0045)]	high
6/27/2024	[RHEL 8 : pki-core (RHSA-2024:4164)]	high
6/27/2024	[RHEL 9 : pki-core (RHSA-2024:4165)]	high
6/27/2024	[RHEL 8 : python3 (RHSA-2024:4166)]	high
6/27/2024	[Debian dla-3843 : linux-config-5.10 - security update]	high
6/27/2024	[Debian dla-3840 : hyperv-daemons - security update]	high
6/27/2024	[Atlassian Confluence 1.0.1 < 7.19.24 / 7.20.x < 8.5.11 / 8.6.x < 8.9.3 (CONFSERVER-95973)]	high
6/27/2024	[IBM WebSphere eXtreme Scale 8.6.1.0 < 8.6.1.6 (7150045)]	high

Datum	Schwachstelle	Bewertung
6/27/2024	[Debian dla-3842 : linux-config-5.10 - security update]	high
6/27/2024	[Debian dla-3841 : linux-config-5.10 - security update]	high
6/27/2024	[Atlassian Confluence 1.0.1 < 7.19.23 / 7.20.x < 8.5.9 / 8.6.x < 8.9.1 (CONFSERVER-95942)]	high
6/27/2024	[Atlassian Confluence 1.0.1 < 7.19.23 / 7.20.x < 8.5.9 / 8.6.x < 8.9.1 (CONFSERVER-95943)]	high
6/27/2024	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : FontForge vulnerabilities (USN-6856-1)]	high
6/27/2024	[Ubuntu 16.04 LTS / 18.04 LTS : Squid vulnerabilities (USN-6857-1)]	high
6/27/2024	[Atlassian Jira Service Management Data Center and Server < 5.4.21 / 5.12.x < 5.12.8 / 5.15.x < 5.16.0 (JSDSERVER-15309)]	high
6/27/2024	[Debian dla-3845 : dlt-daemon - security update]	high
6/27/2024	[Microsoft Edge (Chromium) < 126.0.2592.81 Multiple Vulnerabilities]	high
6/27/2024	[Debian dsa-5723 : libcolorcorrect5 - security update]	high
6/27/2024	[Ubuntu 14.04 LTS : SQLite vulnerability (USN-5615-3)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Thu, 27 Jun 2024

SimpCMS 0.1 Cross Site Scripting

SimpCMS version 0.1 suffers from a cross site scripting vulnerability.

- Link

—

” “Wed, 26 Jun 2024

Ollama Remote Code Execution

Ollama versions prior to 0.1.34 suffer from a remote code execution vulnerability.

- Link

—

” “Wed, 26 Jun 2024

SolarWinds Platform 2024.1 SR1 Race Condition

SolarWinds Platform version 2024.1 SR1 suffers from a race condition vulnerability.

- Link

—

” “Wed, 26 Jun 2024

Automad 2.0.0-alpha.4 Cross Site Scripting

Automad version 2.0.0-alpha.4 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Wed, 26 Jun 2024

Poultry Farm Management System 1.0 Shell Upload

Poultry Farm Management System version 1.0 remote shell upload exploit. This is a variant of the original discovery of this flaw in this software version by Hejap Zairy in March of 2022.

- Link

—

” “Tue, 25 Jun 2024

Faronics WINSelect Hardcoded Credentials / Bad Permissions / Unhashed Password

Faronics WINSelect versions prior to 8.30.xx.903 suffer from having hardcoded credentials, storing unhashed passwords, and configuration file modification vulnerabilities.

- Link

—

” “Mon, 24 Jun 2024

Netis MW5360 Remote Command Execution

The Netis MW5360 router has a command injection vulnerability via the password parameter on the login page. The vulnerability stems from improper handling of the ”password” parameter within the router’s web interface. The router’s login page authorization can be bypassed by simply deleting the authorization header, leading to the vulnerability. All router firmware versions up to V1.0.1.3442 are vulnerable. Attackers can inject a command in the password parameter, encoded in base64, to exploit the command injection vulnerability. When exploited, this can lead to unauthorized command execution, potentially allowing the attacker to take control of the router.

- Link

—

” “Mon, 24 Jun 2024

Edu-Sharing Arbitrary File Upload

Edu-Sharing suffers from an arbitrary file upload vulnerability. Versions below 8.0.8-RC2, 8.1.4-RC0, and 9.0.0-RC19 are affected.

- Link

—

” “Mon, 24 Jun 2024

Flatboard 3.2 Cross Site Scripting

Flatboard version 3.2 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Mon, 24 Jun 2024

Carbon Forum 5.9.0 Cross Site Request Forgery / SQL Injection

Carbon Forum version 5.9.0 suffers from access control, cross site request forgery, file upload, outdated library, and remote SQL injection vulnerabilities.

- Link

—

” “Mon, 24 Jun 2024

Student Attendance Management System 1.0 SQL Injection

Student Attendance Management System version 1.0 suffers from a remote SQL Injection vulnerability that allows for authentication bypass.

- Link

—

” “Mon, 24 Jun 2024

Paradox IP150 Internet Module 1.40.00 Cross Site Request Forgery

Paradox IP150 Internet Module version 1.40.00 suffers from a cross site request forgery vulnerability.

- Link

—

” “Thu, 20 Jun 2024

TURPENTINE XNU Kernel Buffer Overflow

CVE-2024-27815 is a buffer overflow in the XNU kernel that was reported in sbconcat_mbufs. It was publicly fixed in xnu-10063.121.3, released with macOS 14.5, iOS 17.5, and visionOS 1.2. This bug was introduced in xnu-10002.1.13 (macOS 14.0/ iOS 17.0) and was fixed in xnu-10063.121.3 (macOS 14.5/ iOS 17.5). The bug affects kernels compiled with CONFIG_MBUF_MCACHE.

- Link

—

” “Wed, 19 Jun 2024

Bagisto 2.1.2 Client-Side Template Injection

Bagisto version 2.1.2 suffers from a client-side template injection vulnerability.

- Link

—

” “Wed, 19 Jun 2024

User Registration And Management System 3.2 SQL Injection

User Registration and Management System version 3.2 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Tue, 18 Jun 2024

PHP CGI Argument Injection Remote Code Execution

This Metasploit module exploits a PHP CGI argument injection vulnerability affecting PHP in certain configurations on a Windows target. A vulnerable configuration is locale dependant (such as Chinese or Japanese), such that the Unicode best-fit conversion scheme will unexpectedly convert a soft hyphen (0xAD) into a dash (0x2D) character. Additionally a target web server must be configured to run PHP under CGI mode, or directly expose the PHP binary. This issue has been fixed in PHP 8.3.8 (for the 8.3.x branch), 8.2.20 (for the 8.2.x branch), and 8.1.29 (for the 8.1.x branch). PHP 8.0.x and below are end of life and have note received patches. XAMPP is vulnerable in a default configuration, and we can target the /php-cgi/php-cgi.exe endpoint. To target an explicit .php endpoint (e.g. /index.php), the server must be configured to run PHP scripts in CGI mode.

- Link

—

” “Tue, 18 Jun 2024

Apache OFBiz Forgot Password Directory Traversal

Apache OFBiz versions prior to 18.12.13 are vulnerable to a path traversal vulnerability. The vulnerable endpoint /webtools/control/forgotPassword allows an attacker to access the ProgramExport endpoint which in turn allows for remote code execution in the context of the user running the application.

- Link

—

” “Tue, 18 Jun 2024

PowerVR Out-Of-Bounds Write

PowerVR suffers from an out-of-bounds write of firmware addresses in PVRSRVRGXKickTA3DKM().

- Link

—

” “Tue, 18 Jun 2024

PowerVR Uninitialized Memory Disclosure

PowerVR suffers from an uninitialized memory disclosure and crash due to out-of-bounds reads in hwperf_host_%d stream.

- Link

—

” “Tue, 18 Jun 2024

Microweber 2.0.15 Cross Site Scripting

Microweber version 2.0.15 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 18 Jun 2024

Backdoor.Win32.Plugx MVID-2024-0686 Insecure Permissions

Backdoor.Win32.Plugx malware suffers from an insecure permissions vulnerability.

- Link

—

” “Mon, 17 Jun 2024

SPA-CART CMS 1.9.0.6 Username Enumeration / Business Logic Flaw

SPA-CART CMS version 1.9.0.6 suffers from business logic and user enumeration flaws.

- Link

—

” “Mon, 17 Jun 2024

Payroll Management System 1.0 Remote Code Execution

Payroll Management System version 1.0 suffers from a remote code execution vulnerability.

- Link

—

” “Mon, 17 Jun 2024

WordPress RFC WordPress 6.0.8 Shell Upload

WordPress RFC WordPress plugin version 6.0.8 suffers from a remote shell upload vulnerability.

- Link

—

” “Fri, 14 Jun 2024

Premium Support Tickets For WHMCS 1.2.10 Cross Site Scripting

Premium Support Tickets For WHMCS version 1.2.10 suffers from a cross site scripting vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Wed, 26 Jun 2024

ZDI-24-883: Zen Cart findPluginAdminPage Local File Inclusion Remote Code Execution Vulnerability

- Link

—

” “Tue, 25 Jun 2024

ZDI-24-882: VMware vCenter Server Appliance License Server Uncontrolled Memory Allocation Denial-of-Service Vulnerability

- Link

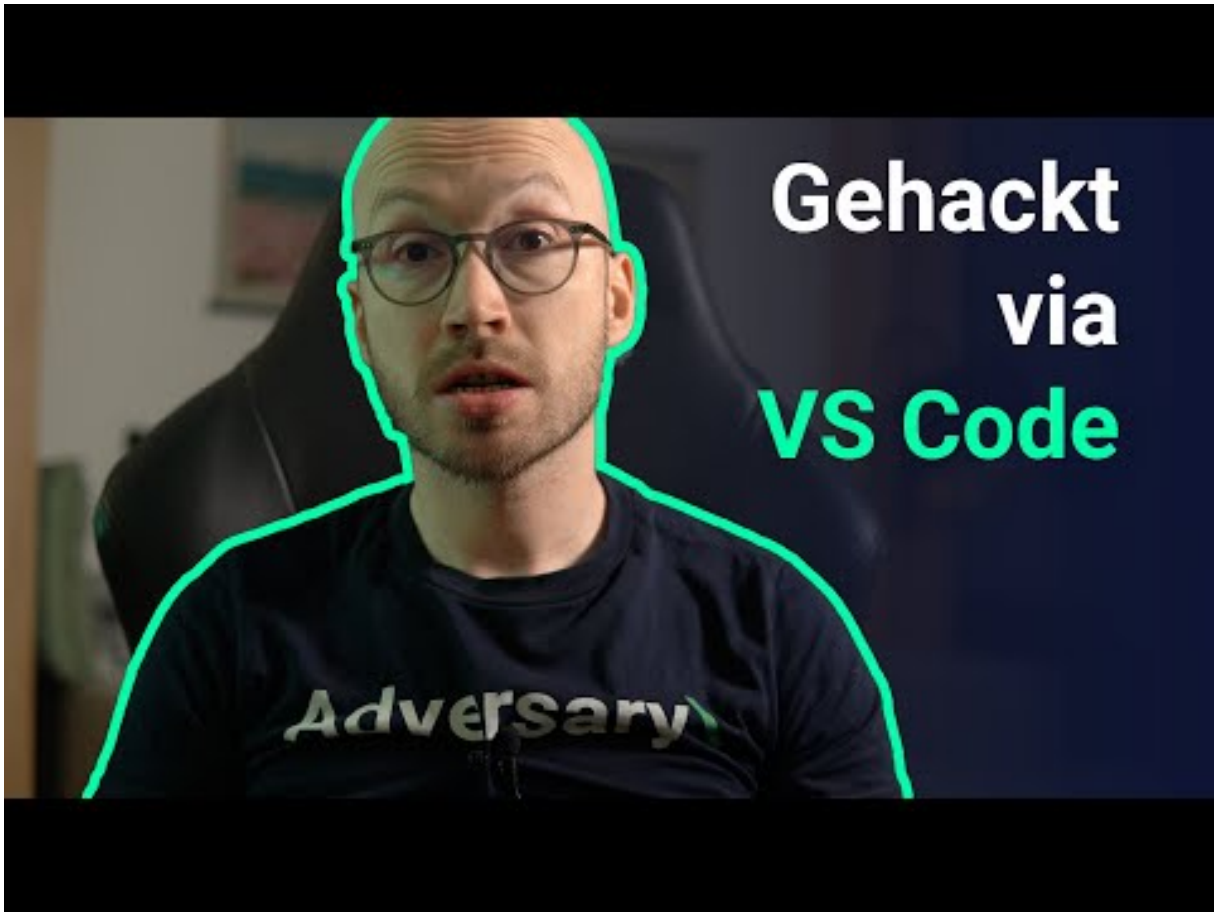
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Die nächste Wahnsinns-Möglichkeit für Angreifer, Software-Unternehmen zu hacken (VSCode Extensions)



Zum Youtube Video

6 Cyberangriffe: (Jun)

Datum	Opfer	Land	Information
2024-06-27	KBC Zagreb	[HRV]	Link
2024-06-25	Cowichan Valley School District	[CAN]	Link
2024-06-24	Sicoob	[BRA]	Link
2024-06-24	Fleury-les-Aubrais	[FRA]	Link
2024-06-24	Acadian Ambulance	[USA]	Link
2024-06-23	Morgunblaðið	[ISL]	Link
2024-06-22	National Health Laboratory Service (NHLS)	[ZAF]	Link
2024-06-22	Agata	[POL]	Link
2024-06-21	DG Immobilien Management (DGIM)	[DEU]	Link
2024-06-20	GIC Housing Finance	[IND]	Link
2024-06-20	Le ministère de la Communication et de l’Information (Kominfo)	[IDN]	Link
2024-06-20	La Scam (Société civile des auteurs multimédia)	[FRA]	Link
2024-06-19	CDK	[USA]	Link
2024-06-19	Olympia Gaming	[USA]	Link
2024-06-18	Hudson school district	[USA]	Link
2024-06-17	MARINA (Maritime Industry Authority)	[PHL]	Link
2024-06-17	Rekah	[ISR]	Link
2024-06-17	Krankenhaus Agatharied	[DEU]	Link
2024-06-16	Oahu Transit Services (OTS)	[USA]	Link
2024-06-16	▯▯▯▯ (Junsi Group) et Brooks Brothers	[HKG]	Link
2024-06-14	GlobalWafers	[TWN]	Link
2024-06-13	Globe Life Inc.	[USA]	Link
2024-06-12	Axido	[FRA]	Link
2024-06-12	Commune de Benalmádena	[ESP]	Link

Datum	Opfer	Land	Information
2024-06-12	Richland School District	[USA]	Link
2024-06-12	Newberg-Dundee School District	[USA]	Link
2024-06-11	Mercatino dell'usato	[ITA]	Link
2024-06-10	Toronto District School Board (TDSB)	[CAN]	Link
2024-06-10	Crown Equipment Corporation	[USA]	Link
2024-06-09	Cleveland	[USA]	Link
2024-06-09	Hands, The Family Network	[CAN]	Link
2024-06-09	Emcali	[COL]	Link
2024-06-08	KADOKAWA	[JPN]	Link
2024-06-08	Mobile County Health Department	[USA]	Link
2024-06-08	Findlay Automotive Group	[USA]	Link
2024-06-06	ASST Rhodense	[ITA]	Link
2024-06-04	Vietnam Post Corporation (Vietnam Post)	[VNM]	Link
2024-06-04	Synnovis	[GBR]	Link
2024-06-04	Groupe IPM	[BEL]	Link
2024-06-02	Institut technologique de Sonora (Itson)	[MEX]	Link
2024-06-02	Special Health Resources (SHR)	[USA]	Link
2024-06-01	Pharmascience	[CAN]	Link

7 Ransomware-Erpressungen: (Jun)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-13	[GBA GROUP]	incransom	Link
2024-06-24	[equinocioplay.com.br]	ransomhub	Link
2024-06-27	[www.cipl.org.in]	ransomhub	Link
2024-06-27	[buyeazzy.com]	darkvault	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-27	[promarkbrands.com]	dAn0n	Link
2024-06-27	[landmarklife.com]	abyss	Link
2024-06-27	[conferenceusa.com]	abyss	Link
2024-06-26	[www.mangimifusco.it]	ransomhub	Link
2024-06-27	[www.cloudeurope.it]	ransomhub	Link
2024-06-23	[coca-cola.com - Myanmar office]	ransomhub	Link
2024-06-26	[daniellegroup.com]	ransomhub	Link
2024-06-26	[Ocasa]	akira	Link
2024-06-26	[Gallos Metal Solutions]	akira	Link
2024-06-27	[KADOKAWA Corporation]	blacksuit	Link
2024-06-26	[GED Lawyers – Sells Open]	arcusmedia	Link
2024-06-26	[Total Revisjon DA]	arcusmedia	Link
2024-06-27	[Ontario West and Bill Blaney Insurance Brokers]	medusa	Link
2024-06-27	[North Coast Petroleum]	medusa	Link
2024-06-27	[Longviewbridge.com]	cloak	Link
2024-06-27	[Ruland-viersen.de]	cloak	Link
2024-06-26	[Waterbury Newton]	akira	Link
2024-06-25	[YKS]	qilin	Link
2024-06-25	[US Dermatology Partners]	bianlian	Link
2024-06-25	[Better Business Bureau]	bianlian	Link
2024-06-25	[PCI Developments]	akira	Link
2024-06-25	[Beckett Thermal Solutions]	akira	Link
2024-06-25	[Utility Datacenter]	akira	Link
2024-06-24	[competenz.co.nz]	lockbit3	Link
2024-06-25	[decreditos.com]	darkvault	Link
2024-06-25	[Planar]	incransom	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-25	[peregrinegp.com (178gb + private SQL_DB 24gb)]	blacksuit	Link
2024-06-25	[rbbschools.net]	blacksuit	Link
2024-06-25	[axiavg.com]	blacksuit	Link
2024-06-25	[catiglass.com]	blacksuit	Link
2024-06-25	[ibewlocal1.org]	blacksuit	Link
2024-06-25	[doityoungs.com]	blacksuit	Link
2024-06-25	[keeservices.com]	blacksuit	Link
2024-06-25	[theeyeclinicsurgicenter.com]	blacksuit	Link
2024-06-25	[sanglier.org.uk]	blacksuit	Link
2024-06-25	[arangobillboard.com]	blacksuit	Link
2024-06-25	[keybenefit.com]	blackbasta	Link
2024-06-25	[scrubsandbeyond.com]	blackbasta	Link
2024-06-25	[tpocc.org]	abyss	Link
2024-06-18	[middletown-township.org]	incransom	Link
2024-06-24	[www.harrisranchbeef.com]	ransomhub	Link
2024-06-24	[www.concisa.eng.br]	qiulong	Link
2024-06-24	[hydmech.com]	cactus	Link
2024-06-24	[westfalia-automotive.com]	cactus	Link
2024-06-24	[Agron (Five Ten) Adidas TERREX]	akira	Link
2024-06-13	[multi-wing.com]	ransomhub	Link
2024-06-17	[bitzsoftwares.com.br]	ransomhub	Link
2024-06-01	[www.sicoob.com.br]	ransomhub	Link
2024-06-24	[Compagnia Trasporti Integrati S.R.L]	monti	Link
2024-06-24	[VTWin.ca]	monti	Link
2024-06-24	[hiawathahomes.org]	blacksuit	Link
2024-06-24	[Revolution Resources]	blacksuit	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-23	[TPI]	play	Link
2024-06-23	[Harvey Construction]	play	Link
2024-06-23	[Belle Tire]	play	Link
2024-06-23	[Hedrick Brothers Construction]	play	Link
2024-06-23	[World inquest]	play	Link
2024-06-23	[Bunger Steel]	play	Link
2024-06-23	[RRCA Accounts Management]	play	Link
2024-06-23	[ProMotion Holdings]	play	Link
2024-06-23	[Custom Concrete]	play	Link
2024-06-23	[federalreserve.gov]	lockbit3	Link
2024-06-23	[Ladco]	play	Link
2024-06-23	[millimages.com]	cactus	Link
2024-06-23	[www.glynmarais.co.za]	cactus	Link
2024-06-23	[hundhausen.de]	cactus	Link
2024-06-23	[fbttransport.com]	cactus	Link
2024-06-23	[daystar.com]	cactus	Link
2024-06-23	[qftemb.com]	lockbit3	Link
2024-06-23	[deskcenter.com]	cactus	Link
2024-06-17	[Tri-City College Prep High School]	medusa	Link
2024-06-17	[Fitzgerald, DePietro & Wojnas CPAs, P.C.]	medusa	Link
2024-06-18	[AJE]	medusa	Link
2024-06-23	[Zerto Security]	handala	Link
2024-06-23	[CIFSOLUTIONS.COM]	clop	Link
2024-06-22	[marvell.com]	lockbit3	Link
2024-06-22	[at-global.com]	lockbit3	Link
2024-06-22	[City of Newburgh]	blackbyte	Link
2024-06-22	[Cityofnewburgh-ny.gov]	blackbyte	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-22	[Erivan Gecom Inc]	rhysida	Link
2024-06-22	[CBIZ, Inc]	meow	Link
2024-06-22	[Greenheck Fan]	meow	Link
2024-06-13	[Maryhaven (MHCLINICAL.LOCAL)]	incransom	Link
2024-06-14	[Ashtons Legal LLP]	qilin	Link
2024-06-21	[Longview Oral & Maxillofacial Surgery]	bianlian	Link
2024-06-21	[MEL aviation Ltd]	bianlian	Link
2024-06-21	[oexpress.id]	darkvault	Link
2024-06-21	[LCS and Partners]	8base	Link
2024-06-21	[Topserve Service Solutions]	8base	Link
2024-06-21	[TC Capital Asia Limited]	8base	Link
2024-06-21	[Wise Construction]	qilin	Link
2024-06-21	[Taiyo Kogyo Co., Ltd.]	8base	Link
2024-06-21	[Hokushinko Co., Ltd.]	8base	Link
2024-06-20	[1234.com]	lockbit3	Link
2024-06-20	[12345.com]	lockbit3	Link
2024-06-20	[www.gbricambi.it [UPDATE]]	ransomhub	Link
2024-06-13	[Sacred Heart Community Service (shcstheheart.org)]	incransom	Link
2024-06-13	[Gorrie-Regan]	incransom	Link
2024-06-20	[Exhaustpro shops]	arcusmedia	Link
2024-06-20	[BankSelfStorage]	arcusmedia	Link
2024-06-20	[GED Lawyers & ..]	arcusmedia	Link
2024-06-18	[Gokals Consumer Electronics & Computers Retail · Fiji]	spacebears	Link
2024-06-18	[Basement Systems]	cicada3301	Link
2024-06-15	[ASST Rhodense]	cicada3301	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-19	[Maintel]	cicada3301	Link
2024-06-19	[Access Group]	cicada3301	Link
2024-06-04	[SAWA INTERNATIONAL]	spacebears	Link
2024-06-18	[Ojai srl]	8base	Link
2024-06-19	[www.invisio.com]	ransomhub	Link
2024-06-19	[Behavioral Health Response (bhr.local)]	incransom	Link
2024-06-19	[Synnovis]	qilin	Link
2024-06-19	[suminoe.us]	cactus	Link
2024-06-19	[Lindermayr]	akira	Link
2024-06-19	[Perfumes & Companhia]	akira	Link
2024-06-19	[First Baptist Medical Center]	moneymessage	Link
2024-06-11	[DERBY SCHOOL]	incransom	Link
2024-06-18	[Circle K Atlanta]	hunters	Link
2024-06-16	[kinslerfamilydentistry]	qilin	Link
2024-06-18	[sofidel.com]	cactus	Link
2024-06-18	[sky-light.com]	cactus	Link
2024-06-18	[reawire.com]	cactus	Link
2024-06-18	[malca-amit.com]	abyss	Link
2024-06-17	[www.gbricambi.it]	ransomhub	Link
2024-06-10	[OCEANAIR]	incransom	Link
2024-06-17	[The Kansas City Kansas Police Department]	blacksuit	Link
2024-06-04	[northcottage.com]	qilin	Link
2024-06-17	[A-Line Staffing Solutions]	underground	Link
2024-06-13	[www.racalacoustics.com [UPDATE]]	ransomhub	Link
2024-06-17	[www.liderit.es]	ransomhub	Link
2024-06-17	[St Vincent de Paul Catholic School]	qilin	Link
2024-06-17	[Sensory Spectrum]	incransom	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-17	[Acteon Group]	hunters	Link
2024-06-17	[pkaufmann.com]	blackbasta	Link
2024-06-17	[modplan.co.uk]	blackbasta	Link
2024-06-17	[wielton.com.pl]	blackbasta	Link
2024-06-17	[grupoamper.com]	blackbasta	Link
2024-06-17	[TETRA Technologies, Inc.]	akira	Link
2024-06-16	[parlorenzo.com]	ransomhub	Link
2024-06-17	[www.domainatcleveland.com]	ransomhub	Link
2024-06-01	[Virum Apotek]	ransomhouse	Link
2024-06-17	[SolidCAM 2024 SP0]	handala	Link
2024-06-17	[Next Step Healthcare]	qilin	Link
2024-06-17	[cosimti.com]	darkvault	Link
2024-06-17	[fifcousa.com]	dAn0n	Link
2024-06-17	[mgfsourcing.com]	blackbasta	Link
2024-06-17	[journohq.com]	darkvault	Link
2024-06-16	[colfax.k12.wi.us]	blacksuit	Link
2024-06-16	[Production Machine & Enterprises]	rhysida	Link
2024-06-16	[CETOS Services]	rhysida	Link
2024-06-15	[Kiemle-Hankins]	rhysida	Link
2024-06-15	[Legrand CRM]	hunters	Link
2024-06-15	[MRI]	hunters	Link
2024-06-15	[Ma’agan Michael Kibbutz]	handala	Link
2024-06-15	[Oahu Transit Services]	dragonforce	Link
2024-06-12	[Sun City Pediatrics PA (USA, TX)]	spacebears	Link
2024-06-11	[Lee Trevino Dental (USA,TX)]	spacebears	Link
2024-06-15	[Peregrine Petroleum]	blacksuit	Link
2024-06-15	[Mountjoy]	bianlian	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-14	[svmasonry.com]	qilin	Link
2024-06-14	[MBE CPA]	metaencryptor	Link
2024-06-14	[EnviroApplications]	qilin	Link
2024-06-14	[www.gannons.co.uk]	apt73	Link
2024-06-14	[New Balance Commodities]	akira	Link
2024-06-14	[Victoria Racing Club]	medusa	Link
2024-06-14	[Mundocar.eu]	cloak	Link
2024-06-13	[Cukierski & Associates, LLC]	everest	Link
2024-06-13	[Diogenet S.r.l.]	everest	Link
2024-06-13	[2K Dental]	everest	Link
2024-06-13	[Dordt University]	bianlian	Link
2024-06-13	[Borrer Executive Search]	apt73	Link
2024-06-13	[www.bigalsfoodservice.co.uk]	apt73	Link
2024-06-13	[www.racalacoustics.com]	ransomhub	Link
2024-06-13	[Kito Canada]	incransom	Link
2024-06-11	[Bock & Associates, LLP]	qilin	Link
2024-06-12	[Walder Wyss and Partners]	play	Link
2024-06-12	[Celluphone]	play	Link
2024-06-12	[Me Too Shoes]	play	Link
2024-06-12	[Ab Monsteras Metall]	play	Link
2024-06-12	[Amarilla Gas]	play	Link
2024-06-12	[Aldenhoven]	play	Link
2024-06-12	[ANTECH-GUTLING Gruppe]	play	Link
2024-06-12	[Refcio & Associates]	play	Link
2024-06-12	[City Builders]	play	Link
2024-06-12	[Eurotrol B.V.]	blacksuit	Link
2024-06-12	[Seagulf Marine Industries]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-12	[Western Mechanical]	play	Link
2024-06-12	[Trisun Land Services]	play	Link
2024-06-10	[GEMCO Constructors]	medusa	Link
2024-06-10	[Dynamo Electric]	medusa	Link
2024-06-11	[Farnell Packaging]	medusa	Link
2024-06-12	[hydefuel.com]	qilin	Link
2024-06-12	[Diverse Technology Industrial]	play	Link
2024-06-12	[Air Cleaning Specialists]	play	Link
2024-06-12	[Corbin Turf & Ornamental Supply]	play	Link
2024-06-12	[Kinter]	play	Link
2024-06-12	[Goodman Reichwald-Dodge]	play	Link
2024-06-12	[3GL Technology Solutions]	play	Link
2024-06-12	[Brainworks Software]	play	Link
2024-06-12	[Eagle Materials]	play	Link
2024-06-12	[Great Lakes International Trading]	play	Link
2024-06-12	[Smartweb]	play	Link
2024-06-12	[Peterbilt of Atlanta]	play	Link
2024-06-12	[Chroma Color]	play	Link
2024-06-12	[Shinnick & Ryan]	play	Link
2024-06-12	[ZeepLive]	darkvault	Link
2024-06-12	[Concrete]	hunters	Link
2024-06-12	[IPM Group (Multimedia Information & Production Company)]	akira	Link
2024-06-12	[manncorp.com]	lockbit3	Link
2024-06-12	[sgvfr.com]	trinity	Link
2024-06-12	[CBSTRAINING]	trinity	Link
2024-06-11	[Kutes.com]	redransomware	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-11	[www.novabitsrl.it]	ransomhub	Link
2024-06-11	[smicusa.com]	ransomhub	Link
2024-06-11	[www.ham.org.br]	ransomhub	Link
2024-06-12	[NJORALSURGERY.COM]	clop	Link
2024-06-11	[SolidCAM LEAK]	handala	Link
2024-06-12	[Zuber Gardner CPAs pt.2]	everest	Link
2024-06-09	[Seafrigo]	dragonforce	Link
2024-06-12	[Special Health Resources]	blacksuit	Link
2024-06-11	[WinFashion ERP]	arcusmedia	Link
2024-06-12	[apex.uk.net]	apt73	Link
2024-06-12	[AlphaNovaCapital]	apt73	Link
2024-06-12	[AMI Global Assistance]	apt73	Link
2024-06-06	[filmetrics corporation]	trinity	Link
2024-06-11	[Embotits Espina, SLU]	8base	Link
2024-06-10	[a-agroup]	qilin	Link
2024-06-10	[Harper Industries]	hunters	Link
2024-06-10	[nordspace.lt]	darkvault	Link
2024-06-05	[www.ugrocapital.com]	ransomhub	Link
2024-06-10	[Arge Baustahl]	akira	Link
2024-06-10	[transportlaberge.com]	cactus	Link
2024-06-10	[sanyo-shokai.co.jp]	cactus	Link
2024-06-10	[wave2.co.kr]	darkvault	Link
2024-06-10	[jmthompson.com]	cactus	Link
2024-06-10	[ctsystem.com]	cactus	Link
2024-06-10	[ctgbrands.com]	cactus	Link
2024-06-10	[SolidCAM]	handala	Link
2024-06-08	[EvoEvents]	dragonforce	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-08	[Barrett Eye Care]	dragonforce	Link
2024-06-08	[Parrish-McCall Constructors]	dragonforce	Link
2024-06-08	[California Rice Exchange]	rhysida	Link
2024-06-07	[Allied Toyota Lift]	qilin	Link
2024-06-08	[Hoppecke]	dragonforce	Link
2024-06-07	[Elite Limousine Plus Inc]	bianlian	Link
2024-06-07	[ccmaui.org]	lockbit3	Link
2024-06-07	[talalayglobal.com]	blackbasta	Link
2024-06-07	[akdenizchemson.com]	blackbasta	Link
2024-06-07	[Reinhold Sign Service]	akira	Link
2024-06-07	[Axip Energy Services]	hunters	Link
2024-06-06	[RAVEN Mechanical]	hunters	Link
2024-06-06	[dmedelivers.com]	embargo	Link
2024-06-06	[fpr-us.com]	cactus	Link
2024-06-06	[TBMCG.com]	ElDorado	Link
2024-06-06	[www.vet.k-state.edu]	ElDorado	Link
2024-06-06	[www.uccretrievals.com]	ElDorado	Link
2024-06-06	[robson.com]	blackbasta	Link
2024-06-06	[elutia.com]	blackbasta	Link
2024-06-06	[ssiworld.com]	blackbasta	Link
2024-06-06	[driver-group.com]	blackbasta	Link
2024-06-06	[HTE Technologies]	ElDorado	Link
2024-06-06	[goughhomes.com]	ElDorado	Link
2024-06-06	[Baker Triangle]	ElDorado	Link
2024-06-06	[www.tankerska.hr]	ElDorado	Link
2024-06-06	[cityofpensacola.com]	ElDorado	Link
2024-06-06	[thunderbirdcc.org]	ElDorado	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-06	[www.itasnatta.edu.it]	ElDorado	Link
2024-06-06	[panzersolutions.com]	ElDorado	Link
2024-06-06	[lindostar.it]	ElDorado	Link
2024-06-06	[burotec.biz]	ElDorado	Link
2024-06-06	[celplan.com]	ElDorado	Link
2024-06-06	[adamshomes.com]	ElDorado	Link
2024-06-06	[dynasafe.com]	blackbasta	Link
2024-06-06	[Panasonic Australia]	akira	Link
2024-06-04	[Health People]	medusa	Link
2024-06-04	[IPPBX]	medusa	Link
2024-06-04	[Market Pioneer International Corp]	medusa	Link
2024-06-04	[Mercy Drive Inc]	medusa	Link
2024-06-04	[Radiosurgery New York]	medusa	Link
2024-06-04	[Inside Broadway]	medusa	Link
2024-06-04	[Oracle Advisory Services]	medusa	Link
2024-06-04	[Women’s Sports Foundation]	medusa	Link
2024-06-05	[“Moshe Kahn Advocates”]	mallox	Link
2024-06-05	[craigsteven.com]	lockbit3	Link
2024-06-05	[Elfi-Tech]	handala	Link
2024-06-05	[Dubai Municipality (UAE)]	daixin	Link
2024-06-05	[E-T-A]	akira	Link
2024-06-01	[Frontier.com]	ransomhub	Link
2024-06-04	[Premium Broking House]	SenSayQ	Link
2024-06-04	[Vimer Industrie Grafiche Italiane]	SenSayQ	Link
2024-06-04	[Voorhees Family Office Services]	everest	Link
2024-06-04	[Mahindra Racing]	akira	Link
2024-06-04	[naprodgroup.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-03	[Madata Data Collection & Internet Portals]	mallox	Link
2024-06-03	[Río Negro]	mallox	Link
2024-06-03	[Langescheid GbR]	arcusmedia	Link
2024-06-03	[Franja IT Integradores de Tecnología]	arcusmedia	Link
2024-06-03	[Duque Saldarriaga]	arcusmedia	Link
2024-06-03	[BHMAC]	arcusmedia	Link
2024-06-03	[Botselo]	arcusmedia	Link
2024-06-03	[Immediate Transport – UK]	arcusmedia	Link
2024-06-01	[cfymca.org]	lockbit3	Link
2024-06-03	[Northern Minerals Limited]	bianlian	Link
2024-06-03	[ISETO CORPORATION]	8base	Link
2024-06-03	[Nidec Motor Corporation]	8base	Link
2024-06-03	[Anderson Mikos Architects]	akira	Link
2024-06-03	[My City application]	handala	Link
2024-06-02	[www.eastshoresound.com]	ransomhub	Link
2024-06-02	[smithandcaugheys.co.nz]	lockbit3	Link
2024-06-01	[Frontier]	ransomhub	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.