Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240623

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

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

—

Sicherheitsupdates: Root-Lücke bedroht VMware vCenter Server

Unter anderem zwei kritische Schwachstellen bedrohen vCenter Server und Cloud Foundation von VMware.

- Link

—

CISA warnt: Angriffe auf kritische Lücke in Progress Telerik Report Server

In der Berichtsverwaltung Progress Telerik Report Server greifen Kriminelle eine Sicherheitslücke an. Sie erlaubt die Umgehung der Authentifizierung.

- Link

—

Nextcloud: Angreifer können Zwei-Faktor-Authentifizierung umgehen

Die Clouddienst-Software Nextcloud ist verwundbar. In aktuellen Versionen haben die Entwickler mehrere Sicherheitslücken geschlossen.

- Link

—

Ivanti Endpoint Manager: Exploit für kritische Lücke aufgetaucht

Ein Proof-of-Concept-Exploit für eine kritische Lücke in Ivanti Endpoint Manager ist aufgetaucht. Zudem gibt es ein Update für den Hotfix.

- Link

—

Sicherheitsupdates: Angreifer können Asus-Router kompromittieren

Mehrere WLAN-Router von Asus sind verwundbar und Angreifer können auf sie zugreifen. Updates lösen mehrere Sicherheitsprobleme.

- Link

—

BIOS-Lücken: Angreifer können Dell-PCs kompromittieren

Unter anderem PCs der Serie Alienware und Inspiron sind vor Attacken gefährdet. Dabei kann Schadcode auf Computer gelangen.

- Link

—

CISA warnt: Kritischer PHP-Bug wird von Ransomware ausgenutzt

Automatisierte Attacken gegen Windows-Systeme mit PHP-CGI führen zur Infektion. Die Angreifer laden Schadcode nach und verschlüsseln den Server.

- 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	0.958120000	0.994570000	Link
CVE-2023-6553	0.928510000	0.990390000	Link
CVE-2023-5360	0.911260000	0.988790000	Link
CVE-2023-4966	0.971290000	0.998020000	Link
CVE-2023-48795	0.961680000	0.995220000	Link
CVE-2023-47246	0.943030000	0.992030000	Link
CVE-2023-46805	0.955460000	0.994120000	Link
CVE-2023-46747	0.972480000	0.998480000	Link
CVE-2023-46604	0.931360000	0.990710000	Link
CVE-2023-4542	0.924200000	0.989940000	Link
CVE-2023-43208	0.959780000	0.994850000	Link
CVE-2023-43177	0.960230000	0.994920000	Link
CVE-2023-42793	0.970430000	0.997640000	Link
CVE-2023-41265	0.920320000	0.989490000	Link
CVE-2023-39143	0.948440000	0.992940000	Link
CVE-2023-38205	0.945440000	0.992420000	Link
CVE-2023-38203	0.968820000	0.997160000	Link
CVE-2023-38146	0.905210000	0.988360000	Link
CVE-2023-38035	0.974870000	0.999740000	Link
CVE-2023-36845	0.966580000	0.996460000	Link
CVE-2023-3519	0.912170000	0.988860000	Link
CVE-2023-35082	0.967870000	0.996900000	Link
CVE-2023-35078	0.967810000	0.996870000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34993	0.971260000	0.998010000	Link
CVE-2023-34960	0.922260000	0.989680000	Link
CVE-2023-34634	0.920590000	0.989530000	Link
CVE-2023-34468	0.906650000	0.988450000	Link
CVE-2023-34362	0.957100000	0.994400000	Link
CVE-2023-34039	0.944630000	0.992290000	Link
CVE-2023-3368	0.931130000	0.990680000	Link
CVE-2023-33246	0.972320000	0.998460000	Link
CVE-2023-32315	0.973460000	0.998970000	Link
CVE-2023-30625	0.938290000	0.991450000	Link
CVE-2023-30013	0.962250000	0.995310000	Link
CVE-2023-29300	0.969840000	0.997460000	Link
CVE-2023-29298	0.943950000	0.992160000	Link
CVE-2023-28771	0.918640000	0.989380000	Link
CVE-2023-28121	0.923740000	0.989840000	Link
CVE-2023-27524	0.970400000	0.997620000	Link
CVE-2023-27372	0.973630000	0.999040000	Link
CVE-2023-27350	0.971140000	0.997940000	Link
CVE-2023-26469	0.932230000	0.990820000	Link
CVE-2023-26360	0.952190000	0.993540000	Link
CVE-2023-26035	0.965720000	0.996230000	Link
CVE-2023-25717	0.956860000	0.994350000	Link
CVE-2023-25194	0.967930000	0.996930000	Link
CVE-2023-2479	0.963760000	0.995710000	Link
CVE-2023-24489	0.973550000	0.999010000	Link
CVE-2023-23752	0.948880000	0.993020000	Link
CVE-2023-23397	0.915470000	0.989130000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23333	0.963260000	0.995590000	Link
CVE-2023-22527	0.972640000	0.998540000	Link
CVE-2023-22518	0.965950000	0.996280000	Link
CVE-2023-22515	0.973330000	0.998890000	Link
CVE-2023-21839	0.955020000	0.994020000	Link
CVE-2023-21554	0.950840000	0.993320000	Link
CVE-2023-20887	0.966680000	0.996490000	Link
CVE-2023-1671	0.964510000	0.995860000	Link
CVE-2023-0669	0.968870000	0.997170000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 21 Jun 2024

[UPDATE] [hoch] GStreamer: Schwachstelle ermöglicht Codeausführung oder Denial-of-Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in GStreamer ausnutzen, um beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Fri, 21 Jun 2024

[UPDATE] [hoch] Mozilla Firefox: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Firefox ESR ausnutzen, um beliebigen Code auszuführen, um einen Denial of Service Zustand herbeizuführen und um Sicherheitsmechanismen zu umgehen, sowie den Benutzer zu täuschen.

- Link

—

Fri, 21 Jun 2024

[NEU] [hoch] IBM WebSphere Application Server: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in IBM WebSphere Application Server ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Fri, 21 Jun 2024

[NEU] [hoch] xwiki: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit Administratorrechten

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in xwiki ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen.

- Link

—

Fri, 21 Jun 2024

[NEU] [hoch] Moodle: Schwachstelle ermöglicht Cross Site Scripting

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Moodle ausnutzen, um einen Cross Site Scripting Angriff durchzuführen.

- Link

—

Fri, 21 Jun 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu erzeugen, Sicherheitsmechanismen zu umgehen und möglicherweise andere nicht spezifizierte Auswirkungen zu haben.

- Link

—

Fri, 21 Jun 2024

[UPDATE] [hoch] SolarWinds Serv-U Managed File Transfer Server: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in SolarWinds Serv-U Managed File Transfer Server ausnutzen, um Informationen offenzulegen.

- Link

—

Fri, 21 Jun 2024

[UPDATE] [kritisch] Adobe Magento Open Source: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Adobe Magento ausnutzen, um beliebigen Programmcode auszuführen, um seine Privilegien zu erhöhen und die Sicherheitsmaßnahmen zu umgehen.

- Link

—

Fri, 21 Jun 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder um Sicherheitsmaßnahmen zu umgehen.

- Link

—

Fri, 21 Jun 2024

[UPDATE] [hoch] PuTTY: Schwachstelle ermöglicht Erlangen des privaten Schlüssels

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PuTTY und Anwendungen, die PuTTY nutzen, wie z.B. FileZilla, WinSCP und TortoiseGit ausnutzen, um bei 521-bit ECDSA den privaten Schlüssel des Nutzers zu erlangen.

- Link

—

Fri, 21 Jun 2024

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um beliebigen Programmcode auszuführen und um Sicherheitsmechanismen zu umgehen.

- Link

—

Fri, 21 Jun 2024

[UPDATE] [hoch] Ghostscript: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Ghostscript ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen.

- Link

—

Thu, 20 Jun 2024

[NEU] [hoch] Apache Superset: Schwachstelle ermöglicht Manipulation und Offenlegung von Daten

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Apache Superset ausnutzen, um Daten zu manipulieren und offenzulegen.

- Link

—

Thu, 20 Jun 2024

[NEU] [hoch] VMware Tanzu Spring Cloud Skipper: Schwachstelle ermöglicht Manipulation von Dateien

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in VMware Tanzu Spring Cloud Skipper ausnutzen, um Dateien zu manipulieren.

- Link

—

Thu, 20 Jun 2024

[NEU] [hoch] IGEL OS: Mehrere Schwachstellen ermöglichen Codeausführung

Ein lokaler Angreifer kann mehrere Schwachstellen in IGEL OS ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 20 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, 20 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

—

Thu, 20 Jun 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

—

Thu, 20 Jun 2024

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

Ein Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um Dateien zu manipulieren, einen Denial-of-Service-Zustand zu verursachen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, seine Privilegien zu erweitern oder um weitere nicht spezifizierte Angriffe auszuführen.

- Link

—

Wed, 19 Jun 2024

[UPDATE] [hoch] GNU libc: mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in GNU libc ausnutzen, um beliebigen Programmcode mit den Rechten des Angegriffenen auszuführen oder einen Denial of Service Angriff durchführen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
6/22/2024	[SUSE SLES15 Security Update : rmt-server (SUSE-SU-2024:2140-1)]	critical
6/22/2024	[GLSA-202406-05 : JHead: Multiple Vulnerabilities]	critical
6/22/2024	[GLSA-202406-04 : LZ4: Memory Corruption]	critical
6/21/2024	[Ivanti Endpoint Manager < 2022 SU4 Privilege Escalation (SA-2023-06-20)]	critical
6/21/2024	[Ivanti Endpoint Manager < 2022 SU3 Privilege Escalation (SA-2023-06-06)]	critical
6/22/2024	[SUSE SLES15 Security Update : kernel (Live Patch 24 for SLE 15 SP4) (SUSE-SU-2024:2163-1)]	high
6/22/2024	[SUSE SLES15 Security Update : kernel (Live Patch 20 for SLE 15 SP4) (SUSE-SU-2024:2160-1)]	high
6/22/2024	[SUSE SLES12 / SLES15 Security Update : kernel (Live Patch 41 for SLE 15 SP2) (SUSE-SU-2024:2123-1)]	high
6/22/2024	[SUSE SLES15 Security Update : kernel (Live Patch 38 for SLE 15 SP2) (SUSE-SU-2024:2109-1)]	high
6/22/2024	[SUSE SLES15 Security Update : kernel (Live Patch 39 for SLE 15 SP3) (SUSE-SU-2024:2145-1)]	high
6/22/2024	[SUSE SLES12 Security Update : kernel (Live Patch 56 for SLE 12 SP5) (SUSE-SU-2024:2147-1)]	high
6/22/2024	[SUSE SLES15 Security Update : kernel (Live Patch 44 for SLE 15 SP3) (SUSE-SU-2024:2149-1)]	high
6/22/2024	[SUSE SLES12 Security Update : vte (SUSE-SU-2024:2151-1)]	high
6/22/2024	[SUSE SLES15 Security Update : kernel (Live Patch 43 for SLE 15 SP3) (SUSE-SU-2024:2139-1)]	high

Datum	Schwachstelle	Bewertung
6/22/2024	[SUSE SLES12 Security Update : kernel (Live Patch 54 for SLE 12 SP5) (SUSE-SU-2024:2130-1)]	high
6/22/2024	[SUSE SLES15 Security Update : kernel (Live Patch 19 for SLE 15 SP4) (SUSE-SU-2024:2165-1)]	high
6/22/2024	[SUSE SLES15 Security Update : kernel (Live Patch 13 for SLE 15 SP4) (SUSE-SU-2024:2156-1)]	high
6/22/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : python-cryptography (SUSE-SU-2024:2138-1)]	high
6/22/2024	[SUSE SLES15 Security Update : kernel (Live Patch 42 for SLE 15 SP3) (SUSE-SU-2024:2148-1)]	high
6/22/2024	[SUSE SLES12 / SLES15 Security Update : kernel (Live Patch 33 for SLE 15 SP3) (SUSE-SU-2024:2124-1)]	high
6/22/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : vte (SUSE-SU-2024:2153-1)]	high
6/22/2024	[SUSE SLES15 / openSUSE 15 Security Update : podofo (SUSE-SU-2024:2137-1)]	high
6/22/2024	[SUSE SLES15 Security Update : kernel (Live Patch 23 for SLE 15 SP4) (SUSE-SU-2024:2162-1)]	high
6/22/2024	[SUSE SLES15 Security Update : kernel (Live Patch 47 for SLE 15 SP2) (SUSE-SU-2024:2121-1)]	high
6/22/2024	[SUSE SLES15 Security Update : kernel (Live Patch 43 for SLE 15 SP2) (SUSE-SU-2024:2115-1)]	high
6/22/2024	[SUSE SLES15 Security Update : vte (SUSE-SU-2024:2152-1)]	high
6/22/2024	[SUSE SLES15 Security Update : kernel (Live Patch 15 for SLE 15 SP4) (SUSE-SU-2024:2164-1)]	high
6/22/2024	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2024:2135-1)]	high
6/22/2024	[SUSE SLES15 Security Update : kernel (Live Patch 37 for SLE 15 SP3) (SUSE-SU-2024:2143-1)]	high
6/22/2024	[SUSE SLES15 Security Update : kernel (Live Patch 46 for SLE 15 SP2) (SUSE-SU-2024:2120-1)]	high

Datum	Schwachstelle	Bewertung
6/22/2024	[SUSE SLES15 Security Update : kernel (Live Patch 21 for SLE 15 SP4) (SUSE-SU-2024:2166-1)]	high
6/22/2024	[RHEL 6 : quarkus-core (Unpatched Vulnerability)]	high
6/22/2024	[GLSA-202406-02 : Flatpak: Sandbox Escape]	high
6/22/2024	[Slackware Linux 15.0 / current emacs Vulnerability (SSA:2024-174-01)]	high
6/21/2024	[FreeBSD : qt5-webengine – Multiple vulnerabilities (aa2b65e4-2f63-11ef-9cab-4ccc6adda413)]	high
6/21/2024	[FreeBSD : openvpn – two security fixes (142c538e-b18f-40a1-afac-c479effadd5c)]	high
6/21/2024	[FreeBSD : chromium – multiple security fixes (007e7e77-2f06-11ef-8a0f-a8a1599412c6)]	high
6/21/2024	[FreeBSD : qt6-webengine – Multiple vulnerabilities (c5415838-2f52-11ef-9cab-4ccc6adda413)]	high
6/21/2024	[Fedora 40 : chromium (2024-d2b54d5a9d)]	high
6/21/2024	[Oracle Linux 8 : thunderbird (ELSA-2024-4036)]	high
6/21/2024	[CentOS 7 : thunderbird (RHSA-2024:4016)]	high
6/21/2024	[Fedora 39 : webkitgtk (2024-826bf5a09a)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“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

—

” “Fri, 14 Jun 2024

AEGON LIFE 1.0 Cross Site Scripting

AEGON LIFE version 1.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Fri, 14 Jun 2024

AEGON LIFE 1.0 Remote Code Execution

AEGON LIFE version 1.0 suffers from an unauthenticated remote code execution vulnerability.

- Link

—

” “Fri, 14 Jun 2024

AEGON LIFE 1.0 SQL Injection

AEGON LIFE version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Fri, 14 Jun 2024

PHP Remote Code Execution

PHP versions prior to 8.3.8 suffer from a remote code execution vulnerability.

- Link

—

” “Thu, 13 Jun 2024

Telerik Report Server Authentication Bypass / Remote Code Execution

This Metasploit module chains an authentication bypass vulnerability with a deserialization vulnerability to obtain remote code execution against Telerik Report Server versions 10.0.24.130 and below. The authentication bypass flaw allows an unauthenticated user to create a new user with administrative privileges. The USERNAME datastore option can be used to authenticate with an existing account to prevent the creation of a new one. The deserialization flaw works by uploading a specially crafted report that when loaded will execute an OS command as NT AUTHORITY\SYSTEM. The module will automatically delete the created report but not the account because users are unable to delete themselves.

- Link

—

” “Thu, 13 Jun 2024

Rejetto HTTP File Server (HFS) Unauthenticated Remote Code Execution

The Rejetto HTTP File Server (HFS) version 2.x is vulnerable to an unauthenticated server side template injection (SSTI) vulnerability. A remote unauthenticated attacker can execute code with the privileges of the user account running the HFS.exe server process. This exploit has been tested to work against version 2.4.0 RC7 and 2.3m. The Rejetto HTTP File Server (HFS) version 2.x is no longer supported by the maintainers and no patch is available. Users are recommended to upgrade to newer supported versions.

- Link

—

” “Thu, 13 Jun 2024

Cacti Import Packages Remote Code Execution

This exploit module leverages an arbitrary file write vulnerability in Cacti versions prior to 1.2.27 to achieve remote code execution. It abuses the Import Packages feature to upload a specially crafted package that embeds a PHP file. Cacti will extract this file to an accessible location. The module finally triggers the payload to execute arbitrary PHP code in the context of the user running the web server. Authentication is needed and the account must have access to the Import Packages feature. This is granted by setting the Import Templates permission in the Template Editor section.

- Link

—

” “Thu, 13 Jun 2024

Lost And Found Information System 1.0 Cross Site Scripting

Lost and Found Information System version 1.0 suffers from a reflective cross site scripting vulnerability.

- Link

—

” “Thu, 13 Jun 2024

Lost And Found Information System 1.0 SQL Injection

Lost and Found Information System version 1.0 suffers from an unauthenticated blind boolean-based remote SQL injection vulnerability.

- Link

—

” “Thu, 13 Jun 2024

Lost And Found Information System 1.0 SQL Injection

Lost and Found Information System version 1.0 suffers from an unauthenticated blind time-based remote SQL injection vulnerability.

- Link

—

” “Thu, 13 Jun 2024

Lost And Found Information System 1.0 Cross Site Scripting

Lost and Found Information System version 1.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Thu, 13 Jun 2024

Quick Cart 6.7 Shell Upload

Quick Cart version 6.7 suffers from a remote shell upload vulnerability provided you have administra-

tive privileges.
- Link
—
”

4.2 0-Days der letzten 5 Tage

“Fri, 21 Jun 2024
ZDI-24-881: (Pwn2Own) Ubiquiti Networks EV Station setDebugPortEnabled Exposed Dangerous Method Remote Code Execution Vulnerability
- Link
—
” “Fri, 21 Jun 2024
ZDI-24-880: (Pwn2Own) Ubiquiti Networks EV Station EVCLauncher Improper Certificate Validation Vulnerability
- Link
—
” “Fri, 21 Jun 2024
ZDI-24-879: (Pwn2Own) Ubiquiti Networks EV Station changeUserPassword Missing Authentication Remote Code Execution Vulnerability
- Link
—
” “Fri, 21 Jun 2024
ZDI-24-878: Sony XAV-AX5500 Insufficient Verification of Data Authenticity Remote Code Execution Vulnerability
- Link
—
” “Fri, 21 Jun 2024
ZDI-24-877: (Pwn2Own) Sony XAV-AX5500 CarPlay TLV Stack-based Buffer Overflow Remote Code Execution Vulnerability
- Link
—
” “Fri, 21 Jun 2024
ZDI-24-876: (Pwn2Own) Sony XAV-AX5500 USB Configuration Descriptor Buffer Overflow Remote Code Execution Vulnerability
- Link
—
” “Fri, 21 Jun 2024

ZDI-24-875: (Pwn2Own) Sony XAV-AX5500 WMV/ASF Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-874: (Pwn2Own) Sony XAV-AX5500 Insufficient Firmware Update Validation Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-873: (Pwn2Own) Silicon Labs Gecko OS HTTP GET Request Handling Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-872: (Pwn2Own) Silicon Labs Gecko OS DNS Response Processing Infinite Loop Denial-of-Service Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-871: (Pwn2Own) Silicon Labs Gecko OS HTTP Request Handling Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-870: (Pwn2Own) Silicon Labs Gecko OS http_download Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-869: (Pwn2Own) Silicon Labs Gecko OS Debug Interface Format String Information Disclosure Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-868: (Pwn2Own) Silicon Labs Gecko OS Debug Interface Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-867: (Pwn2Own) Phoenix Contact CHARX SEC-3100 CharxUpdateAgent Unrestricted File Upload Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-866: (Pwn2Own) Phoenix Contact CHARX SEC-3100 CANopenDevice Null Pointer Dereference Denial-of-Service Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-865: Phoenix Contact CHARX SEC-3100 charx_pack_logs Improper Input Validation Local Privilege Escalation Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-864: (Pwn2Own) Phoenix Contact CHARX SEC-3100 OCPP Protocol UpdateFirmware Command Injection Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-863: (Pwn2Own) Phoenix Contact CHARX SEC-3100 plctool Improper Privilege Management Local Privilege Escalation Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-862: (Pwn2Own) Phoenix Contact CHARX SEC-3100 MQTT Protocol JSON Parsing Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-861: (Pwn2Own) Phoenix Contact CHARX SEC-3100 ClientSession Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-860: (Pwn2Own) Phoenix Contact CHARX SEC-3100 HomePlug Protocol Out-Of-Bounds

Read Information Disclosure Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-859: (Pwn2Own) Phoenix Contact CHARX SEC-3100 MTQQ Protocol JSON Parsing Type Confusion Information Disclosure Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-858: (Pwn2Own) Phoenix Contact CHARX SEC-3100 OCPP Protocol Missing Encryption Authentication Bypass Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-857: (Pwn2Own) Phoenix Contact CHARX SEC-3100 Improper Access Control Firewall Bypass Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-856: (Pwn2Own) Phoenix Contact CHARX SEC-3100 Config Manager Improper Input Validation Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-855: (Pwn2Own) Phoenix Contact CHARX SEC-3100 OCPP Protocol Improper Log Output Neutralization Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-854: (Pwn2Own) Autel MaxiCharger AC Elite Business C50 DLB_HostHeartBeat Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-853: (Pwn2Own) Autel MaxiCharger AC Elite Business C50 WebSocket Base64 Decoding Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-852: (Pwn2Own) Autel MaxiCharger AC Elite Business C50 BLE Hardcoded Credentials Authentication Bypass Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-851: (Pwn2Own) Autel MaxiCharger AC Elite Business C50 BLE AppChargingControl Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-850: (Pwn2Own) Alpine Halo9 Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-849: (Pwn2Own) Alpine Halo9 UPDM_wemCmdUpdFSpeDecomp Command Injection Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-848: (Pwn2Own) Alpine Halo9 DecodeUTF7 Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-847: (Pwn2Own) Alpine Halo9 Missing Authentication Information Disclosure Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-846: (Pwn2Own) Alpine Halo9 UPDM_wemCmdCreatSHA256Hash Command Injection Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-845: (Pwn2Own) Alpine Halo9 Improper Verification of Cryptographic Signature Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-844: (Pwn2Own) Alpine Halo9 prh_l2_sar_data_ind Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-843: Linux Kernel USB/IP VHCI Driver Race Condition Privilege Escalation Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-842: Linux Kernel ICMPv6 Router Advertisement Race Condition Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-841: (0Day) Zope CMFCore Uncontrolled Resource Consumption Denial-of-Service Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-840: (Pwn2Own) Wyze Cam v3 TCP Traffic Handling Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-839: (Pwn2Own) Wyze Cam v3 Cloud Infrastructure Improper Authentication Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-838: (Pwn2Own) Wyze Cam v3 Wi-Fi SSID OS Command Injection Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-837: (Pwn2Own) Wyze Cam v3 Realtek Wi-Fi Driver Heap-Based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-836: (Pwn2Own) Synology BC500 update_ntp_config Command Injection Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-835: (Pwn2Own) Synology BC500 Protection Mechanism Failure Software Downgrade Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-834: (Pwn2Own) Synology BC500 Improper Compartmentalization Local Privilege Escalation Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-833: (Pwn2Own) Synology BC500 synocam_param.cgi Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-832: (Pwn2Own) Synology RT6600ax Improper Access Control Firewall Bypass Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-831: (Pwn2Own) Samsung Galaxy S23 Galaxy Store Deeplink Permissive List of Allowed Inputs Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-830: (Pwn2Own) Samsung Galaxy S23 Instant Plays Improper Input Validation Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-829: (Pwn2Own) Samsung Galaxy S23 McsWebViewActivity Permissive List of Allowed Inputs Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-828: (Pwn2Own) Samsung Galaxy S23 instantgame Improper Input Validation Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-827: (Pwn2Own) QNAP TS-464 username Command Injection Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-826: (Pwn2Own) QNAP TS-464 Improper Validation Authentication Bypass Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-825: (Pwn2Own) QNAP TS-464 Log Upload Command Injection Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-824: (Pwn2Own) QNAP TS-464 Cloud Utility Command Injection Remote Code Execution Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-823: (Pwn2Own) QNAP TS-464 TURN Server create_session Server-Side Request Forgery Vulnerability

- Link

—

” “Fri, 21 Jun 2024

ZDI-24-822: (Pwn2Own) HP Color LaserJet Pro MFP 4301fdw CFF Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Thu, 20 Jun 2024

ZDI-24-821: Linux Kernel TIPC Message Reassembly Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 20 Jun 2024

ZDI-24-820: Windscribe Directory Traversal Local Privilege Escalation Vulnerability

- Link

—

” “Thu, 20 Jun 2024

ZDI-24-819: VIPRE Advanced Security Incorrect Permission Assignment Local Privilege Escalation Vulnerability

- Link

—

” “Thu, 20 Jun 2024

ZDI-24-818: VIPRE Advanced Security PMAgent Uncontrolled Search Path Element Local Privilege Escalation Vulnerability

- Link

—

” “Thu, 20 Jun 2024

ZDI-24-817: VIPRE Advanced Security PMAgent Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Thu, 20 Jun 2024

ZDI-24-816: Microsoft Windows Menu DC Bitmap Use-After-Free Local Privilege Escalation Vulnerability

- Link

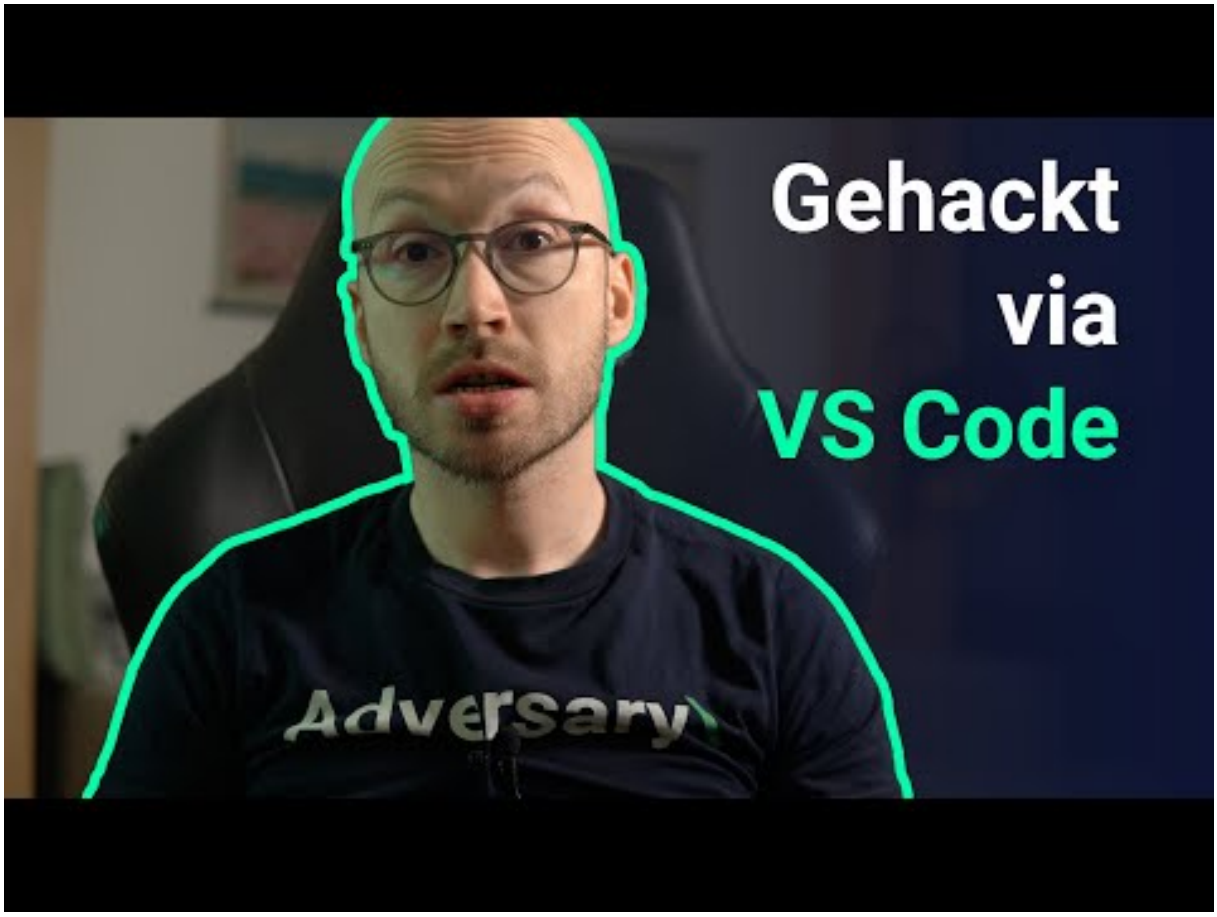
—

”

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
2024-06-21	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
2024-06-17	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
2024-06-12	Richland 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

Datum	Opfer	Land	Information
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

7 Ransomware-Erpressungen: (Jun)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-22	[test123.com]	lockbit3	Link
2024-06-22	[12341.com]	lockbit3	Link
2024-06-22	[1122.com]	lockbit3	Link
2024-06-22	[1133.com]	lockbit3	Link
2024-06-22	[1144.com]	lockbit3	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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.