Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240918

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

Samsung-Druckertreiber ermöglichen Angreifern Rechteausweitung

Für Samsungs Office-Drucker stellt HP einen aktualisierten Universal-Treiber für Windows bereit. Er dichtet ein Rechteausweitungsleck ab.

- Link

—

Angreifer attackieren Sicherheitslücken in Microsofts MSHTML und Whatsup Gold

Die US-amerikanische IT-Sicherheitsbehörde CISA warnt vor Angriffen auf Sicherheitslücken in Microsofts MSHTML und Whatsup Gold.

- Link

—

Sicherheitspatch: Hintertür in einigen D-Link-Routern erlaubt unbefugte Zugriffe

Angreifer können bestimmte Router-Modelle von D-Link attackieren und kompromittieren. Sicherheitsupdates stehen zum Download bereit.

- Link

—

Sicherheitspatch verfügbar: Angriffe auf Ivanti Cloud Service Appliance

Derzeit attackieren Angreifer Ivanti Cloud Service Appliances mit Schadcode. Außedem könnten Attacken auf Endpoint Manager bevorstehen.

- Link

—

Lenovo schließt Lücken in BIOS, Management-Controller und WLAN-Treiber

Wichtige Sicherheitsupdates schützen Computer von Lenovo. Im schlimmsten Fall können Angreifer Schadcode ausführen.

- Link

—

Solarwinds ARM: Unbefugte Zugriffe und Schadcode-Attacken möglich

Die Solarwinds-Entwickler haben zwei Sicherheitslücken in Access Rights Manager geschlossen. Eine Lücke gilt als kritisch.

- Link

—

Sicherheitspatch: Gitlab behebt Lücken in Serverversionen

Angreifer konnten Code einschleusen, fremde Konten übernehmen und den Server außer Gefecht setzen. Admins selbst gehosteter Instanzen sollten patchen.

- Link

—

Cisco: DoS- und Rechteausweitungslücken in IOS und weiteren Produkten

In Ciscos IOS und weiteren Produkten klaffen Sicherheitslücken. Angreifer können ihre Rechte ausweiten oder Geräte lahmlegen.

- Link

—

Ivanti: Updates gegen kritische Lecks im Endpoint Manager und weiteren Produkten

Ivanti bessert Schwachstellen in Endpoint Manager, Workspace Control und Cloud Service Appliance aus. Eine Lücke in EPM erreicht die Höchstwertung CVSS 10.

- Link

—

ownCloud: Update stopft teils hochriskante Sicherheitslücken

Das ownCloud-Projekt warnt vor Sicherheitslücken in der Kollaborationssoftware. Angreifer können etwa Zugriff auf Zugangsdaten erlangen.

- 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	0.957050000	0.994710000	Link
CVE-2023-6895	0.921160000	0.990080000	Link
CVE-2023-6553	0.947820000	0.993070000	Link
CVE-2023-6019	0.918710000	0.989830000	Link
CVE-2023-5360	0.902780000	0.988800000	Link
CVE-2023-52251	0.945480000	0.992720000	Link
CVE-2023-4966	0.970840000	0.998140000	Link
CVE-2023-49103	0.949680000	0.993390000	Link
CVE-2023-48795	0.965330000	0.996440000	Link
CVE-2023-47246	0.961220000	0.995420000	Link
CVE-2023-46805	0.950230000	0.993500000	Link
CVE-2023-46747	0.971020000	0.998240000	Link
CVE-2023-46604	0.969070000	0.997500000	Link
CVE-2023-4542	0.948590000	0.993200000	Link
CVE-2023-43208	0.973740000	0.999270000	Link
CVE-2023-43177	0.961480000	0.995480000	Link
CVE-2023-42793	0.972380000	0.998690000	Link
CVE-2023-41265	0.907590000	0.989090000	Link
CVE-2023-39143	0.940700000	0.992180000	Link
CVE-2023-38205	0.950330000	0.993500000	Link
CVE-2023-38203	0.965830000	0.996580000	Link
CVE-2023-38146	0.920720000	0.990030000	Link
CVE-2023-38035	0.974690000	0.999720000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.966750000	0.996830000	Link
CVE-2023-3519	0.965910000	0.996600000	Link
CVE-2023-35082	0.966710000	0.996820000	Link
CVE-2023-35078	0.970930000	0.998180000	Link
CVE-2023-34993	0.973450000	0.999170000	Link
CVE-2023-34960	0.900520000	0.988650000	Link
CVE-2023-34634	0.923140000	0.990260000	Link
CVE-2023-34362	0.970450000	0.997970000	Link
CVE-2023-34039	0.945100000	0.992670000	Link
CVE-2023-3368	0.939780000	0.992060000	Link
CVE-2023-33246	0.967830000	0.997120000	Link
CVE-2023-32315	0.971490000	0.998400000	Link
CVE-2023-30625	0.953610000	0.994100000	Link
CVE-2023-30013	0.965950000	0.996610000	Link
CVE-2023-29300	0.969240000	0.997540000	Link
CVE-2023-29298	0.970810000	0.998110000	Link
CVE-2023-28432	0.920500000	0.990010000	Link
CVE-2023-28343	0.933130000	0.991340000	Link
CVE-2023-28121	0.925430000	0.990500000	Link
CVE-2023-27524	0.970600000	0.998020000	Link
CVE-2023-27372	0.973930000	0.999350000	Link
CVE-2023-27350	0.969520000	0.997620000	Link
CVE-2023-26469	0.953890000	0.994150000	Link
CVE-2023-26360	0.964390000	0.996120000	Link
CVE-2023-26035	0.968720000	0.997380000	Link
CVE-2023-25717	0.954660000	0.994280000	Link
CVE-2023-25194	0.965150000	0.996360000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963230000	0.995830000	Link
CVE-2023-24489	0.973820000	0.999310000	Link
CVE-2023-23752	0.951460000	0.993660000	Link
CVE-2023-23333	0.960430000	0.995230000	Link
CVE-2023-22527	0.970940000	0.998190000	Link
CVE-2023-22518	0.961800000	0.995550000	Link
CVE-2023-22515	0.973160000	0.999070000	Link
CVE-2023-21839	0.951270000	0.993620000	Link
CVE-2023-21554	0.955880000	0.994500000	Link
CVE-2023-20887	0.970840000	0.998130000	Link
CVE-2023-1671	0.962220000	0.995620000	Link
CVE-2023-0669	0.971300000	0.998350000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 17 Sep 2024

[UPDATE] [kritisch] Ivanti Endpoint Manager: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Ivanti Endpoint Manager ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmaßnahmen zu umgehen, erweiterte Rechte zu erlangen und vertrauliche Informationen preiszugeben.

- Link

—

Tue, 17 Sep 2024

[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen

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

- Link

—

Tue, 17 Sep 2024

[NEU] [hoch] Apple macOS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand herbeizuführen, Spoofing-Angriffe durchzuführen, Daten zu ändern, Sicherheitsmaßnahmen zu umgehen und vertrauliche Informationen offenzulegen

- Link

—

Tue, 17 Sep 2024

[NEU] [hoch] Apple iOS und iPadOS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS ausnutzen, um Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu erzeugen oder vertrauliche Informationen offenzulegen.

- Link

—

Tue, 17 Sep 2024

[NEU] [hoch] Contao: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Contao ausnutzen, um beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.

- Link

—

Tue, 17 Sep 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.

- Link

—

Tue, 17 Sep 2024

[UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, beliebigen Programmcode auszuführen, seine Privilegien zu erweitern, einen Denial of Service Zustand herbeizuführen, Dateien zu manipulieren, Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen oder sonstige Auswirkungen zu verursachen.

- Link

—

Tue, 17 Sep 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu

erhöhen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Tue, 17 Sep 2024

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

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen oder Daten zu manipulieren.

- Link

—

Tue, 17 Sep 2024

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

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

- Link

—

Tue, 17 Sep 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Firefox ESR ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmechanismen zu umgehen, Daten zu manipulieren und den Benutzer zu täuschen.

- Link

—

Tue, 17 Sep 2024

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in PostgreSQL ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Tue, 17 Sep 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 oder Daten zu manipulieren.

- Link

—

Tue, 17 Sep 2024

[UPDATE] [hoch] FreeBSD Project FreeBSD OS: Mehrere Schwachstellen ermöglichen Privilegie-

neskalation und Codeausführung

Ein Angreifer kann mehrere Schwachstellen in FreeBSD Project FreeBSD OS ausnutzen, um seine Privilegien zu erhöhen und beliebigen Code auszuführen.

- Link

—

Tue, 17 Sep 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 ausnutzen oder nicht näher beschriebene Auswirkungen zu erzielen.

- Link

—

Mon, 16 Sep 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

—

Mon, 16 Sep 2024

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

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um seine Privilegien zu erweitern, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen, Informationen offenzulegen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Mon, 16 Sep 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, 16 Sep 2024

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer oder ein lokaler authentifizierter Angreiferkann mehrere Schwachstellen in git ausnutzen, um beliebigen Programmcode auszuführen und und die Sicherheitsmaßnahmen zu umgehen.

- Link

—

Mon, 16 Sep 2024

[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/17/2024	[openSUSE 15 Security Update : htmldoc (openSUSE-SU-2024:0304-1)]	critical
9/17/2024	[openSUSE 15 Security Update : htmldoc (openSUSE-SU-2024:0303-1)]	critical
9/17/2024	[LLama cpp python binding < 0.2.88 Arbitrary Write Vulnerability]	critical
9/17/2024	[RHEL 9 : thunderbird (RHSA-2024:6720)]	critical
9/17/2024	[RHEL 8 : thunderbird (RHSA-2024:6723)]	critical
9/17/2024	[RHEL 8 : thunderbird (RHSA-2024:6721)]	critical
9/17/2024	[RHEL 8 : thunderbird (RHSA-2024:6719)]	critical
9/17/2024	[RHEL 9 : thunderbird (RHSA-2024:6722)]	critical
9/17/2024	[Ubuntu 22.04 LTS : Expat vulnerabilities (USN-7000-2)]	critical
9/17/2024	[Ubuntu 24.04 LTS : xmltok library vulnerabilities (USN-7001-2)]	critical
9/17/2024	[Debian dsa-5770 : expat - security update]	critical
9/17/2024	[Next.js < 14.1.1 Server Actions Server-Side Request Forgery]	high

Datum	Schwachstelle	Bewertung
9/17/2024	[openSUSE 15 Security Update : chromium (openSUSE-SU-2024:0302-1)]	high
9/17/2024	[Fedora 39 : python3.13 (2024-f2fc325c40)]	high
9/17/2024	[Photon OS 3.0: Python3 PHSA-2024-3.0-0795]	high
9/17/2024	[Photon OS 3.0: Linux PHSA-2024-3.0-0795]	high
9/17/2024	[SUSE SLES15 Security Update : 389-ds (SUSE-SU-2024:3257-1)]	high
9/17/2024	[SUSE SLES12 Security Update : kernel (SUSE-SU-2024:3252-1)]	high
9/17/2024	[SUSE SLES15 Security Update : kernel (SUSE-SU-2024:3249-1)]	high
9/17/2024	[SUSE SLED12 / SLES12 Security Update : kernel (SUSE-SU-2024:3251-1)]	high
9/17/2024	[Oracle Linux 8 : pcs (ELSA-2024-6670)]	high
9/17/2024	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : DCMTK vulnerabilities (USN-7010-1)]	high
9/17/2024	[AlmaLinux 8 : pcs (ALSA-2024:6670)]	high
9/17/2024	[Ivanti Endpoint Manager - Cloud Service Appliance < 4.6-519 / 5.0 Command Injection]	high
9/17/2024	[Schneider Electric Accutech Manager Stack Exhaustion (CVE-2024-6918)]	high
9/17/2024	[TeamViewer < 15.51.5 Improper Privilege Management (tv-2024-1001)]	high
9/17/2024	[RHEL 9 : fence-agents (RHSA-2024:6726)]	high
9/17/2024	[Ubuntu 22.04 LTS / 24.04 LTS : FRR vulnerability (USN-7016-1)]	high
9/17/2024	[Ubuntu 20.04 LTS : Quagga vulnerability (USN-7017-1)]	high
9/17/2024	[Debian dla-3890 : galera-4 - security update]	high
9/17/2024	[Google Chrome < 129.0.6668.58 Multiple Vulnerabilities]	high
9/17/2024	[Google Chrome < 129.0.6668.58 Multiple Vulnerabilities]	high

Datum	Schwachstelle	Bewertung
9/17/2024	[Debian dsa-5772 : fonts-opensymbol - security update]	high
9/17/2024	[Debian dsa-5771 : php-twig - security update]	high
9/17/2024	[Amazon Linux AMI : microcode_ctl (ALAS-2024-1946)]	high
9/17/2024	[Oracle Linux 7 : java-1.8.0-openjdk (ELSA-2024-4560)]	high
9/17/2024	[Oracle Linux 7 : ghostscript (ELSA-2024-4549)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Tue, 17 Sep 2024

Microsoft Windows TOCTOU Local Privilege Escalation

CVE-2024-30088 is a Windows kernel elevation of privilege vulnerability which affects many recent versions of Windows 10, Windows 11 and Windows Server 2022. The vulnerability exists inside the function called AuthzBasepCopyoutInternalSecurityAttributes specifically when the kernel copies the _AUTHZBASEP_SECURITY_ATTRIBUTES_INFORMATION of the current token object to user mode. When the kernel performs the copy of the SecurityAttributesList, it sets up the list of the SecurityAttributes structure directly to the user supplied pointed. It then calls RtlCopyUnicodeString and AuthzBasepCopyoutInternalSecurityAttributeValues to copy out the names and values of the SecurityAttribute leading to multiple Time Of Check Time Of Use (TOCTOU) vulnerabilities in the function.

- Link

—

” “Tue, 17 Sep 2024

WordPress LiteSpeed Cache Cookie Theft

This Metasploit module exploits an unauthenticated account takeover vulnerability in LiteSpeed Cache, a WordPress plugin that currently has around 6 million active installations. In LiteSpeed Cache versions prior to 6.5.0.1, when the Debug Logging feature is enabled, the plugin will log admin cookies to the /wp-content/debug.log endpoint which is accessible without authentication. The Debug Logging feature in the plugin is not enabled by default. The admin cookies found in the debug.log can be used to upload and execute a malicious plugin containing a payload.

- Link

—

” “Tue, 17 Sep 2024

GibbonEdu Core 26.0.00 Cross Site Scripting

GibbonEdu Core version 26.0.00 suffers from a cross site scripting vulnerability that can lead to privilege escalation.

- Link

—

” “Tue, 17 Sep 2024

TP-Link Archer AX50 Cross Site Scripting

TP-Link Archer AX50 router with firmware version 1.0.11 build 2022052 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 17 Sep 2024

HTMLy 2.9.9 Cross Site Scripting

HTMLy version 2.9.9 suffers from a persistent cross site scripting vulnerability that can lead to account takeover.

- Link

—

” “Tue, 17 Sep 2024

Dockwatch Remote Command Execution

Dockwatch is a container management web UI for docker. It runs by default without authentication, although guidance is available for how to setup credentials for access. It has a Commands feature that allows a user to run docker commands such as inspect, network, ps. Prior to fix, it did not restrict input for parameters, so both container and parameters for the dockerInspect command were vulnerable to shell command injection on the container as the abc user with (limited) command output. See commits 23df366 and c091e4c for fixes.

- Link

—

” “Tue, 17 Sep 2024

Microsoft SQL Server Masked Data Exposure

Microsoft SQL Server versions 2014, 2016, 2017, 2019, and 2022 suffer from an issue where masked data can be exposed through a brute force attack.

- Link

—

” “Tue, 17 Sep 2024

SPIP BigUp 4.0 Code Injection

SPIP BigUp version 4.0 suffers from a remote PHP code injection vulnerability.

- Link

—

” “Tue, 17 Sep 2024

Online Student Grading System 1.0 Code Injection

Online Student Grading System version 1.0 suffers from a remote PHP code injection vulnerability.

- Link

—

” “Tue, 17 Sep 2024

Online Notice Board System 1.0 Arbitrary File Upload

Online Notice Board System version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Tue, 17 Sep 2024

Online Bus Ticket Booking Website 1.0 Arbitary File Upload

Online Bus Ticket Booking Website version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Tue, 17 Sep 2024

Old Age Home Management System 1.0 Code Injection

Old Age Home Management System version 1.0 suffers from a remote PHP code injection vulnerability.

- Link

—

” “Tue, 17 Sep 2024

Membership Management System 1.0 Code Injection

Membership Management System version 1.0 suffers from a remote PHP code injection vulnerability.

- Link

—

” “Tue, 17 Sep 2024

Live Membership Management System 1.0 Code Injection

Live Membership Management System version 1.0 suffers from a remote PHP code injection vulnerability.

- Link

—

” “Tue, 17 Sep 2024

Expense Management System 1.0 Arbitrary File Upload

Expense Management System version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Tue, 17 Sep 2024

Beauty Parlour And Saloon Management System 1.1 SQL Injection

Beauty Parlour and Saloon Management System version 1.1 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Tue, 17 Sep 2024

Auto/Taxi Stand Management System 1.0 Insecure Settings

Auto/Taxi Stand Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 16 Sep 2024

VICIdial SQL Injection / Remote Code Execution

Proof of concept exploit that allows an attacker to retrieve administrative credentials through SQL injection and ultimately execute arbitrary code on the target server.

- Link

—

” “Mon, 16 Sep 2024

Rejetto HTTP File Server 2.3m Template Injection / Arbitrary Code Execution

Proof of concept remote code execution exploit for Rejetto HTTP File Server (HFS) version 2.3m.

- Link

—

” “Mon, 16 Sep 2024

Calibre 7.14.0 Remote Code Execution

Proof of concept unauthenticated remote code execution exploit for Calibre versions 7.14.0 and below.

- Link

—

” “Mon, 16 Sep 2024

Veeam Backup And Replication 12.1.2.172 Remote Code Execution

Veeam Backup and Replication version 12.1.2.172 unauthenticated remote code execution exploit.

- Link

—

” “Mon, 16 Sep 2024

Ship Ferry Ticket Reservation System 1.0 SQL Injection

Ship Ferry Ticket Reservation System version 1.0 suffers from multiple remote SQL injection vulnerabilities.

- Link

—

” “Mon, 16 Sep 2024

Reservation Management System 1.0 Cross Site Request Forgery

Reservation Management System version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Mon, 16 Sep 2024

Online Job Recruitment Portal Project 1.0 Arbitrary File Upload

Online Job Recruitment Portal Project version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Mon, 16 Sep 2024

IFSC Code Finder Portal 1.0 Insecure Settings

IFSC Code Finder Portal version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Tue, 17 Sep 2024

ZDI-24-1272: PDF-XChange Editor AcroForm Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1271: PDF-XChange Editor AcroForm Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1270: PDF-XChange Editor Doc Object Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1269: PDF-XChange Editor TIF File Parsing Out-Of-Bounds Read Information Disclosure

Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1268: PDF-XChange Editor PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1267: PDF-XChange Editor PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1266: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1265: PDF-XChange Editor RTF File Parsing Uninitialized Variable Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1264: PDF-XChange Editor PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1263: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1262: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1261: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1260: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1259: PDF-XChange Editor TIF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1258: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1257: PDF-XChange Editor TIF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1256: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1255: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1254: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1253: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1252: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1251: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1250: PDF-XChange Editor PPM File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1249: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1248: PDF-XChange Editor PDF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1247: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1246: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1245: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1244: PDF-XChange Editor U3D File Parsing Use-After-Free Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1243: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1242: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1241: PDF-XChange Editor U3D File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1240: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1239: PDF-XChange Editor U3D File Parsing Use-After-Free Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1238: PDF-XChange Editor U3D File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1237: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1236: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1235: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1234: WinZip Mark-of-the-Web Bypass Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1233: Cohesive Networks VNS3 Command Injection Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1232: Cohesive Networks VNS3 Command Injection Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1231: Cohesive Networks VNS3 Command Injection Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1230: Cohesive Networks VNS3 Command Injection Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1229: BlueZ HID over GATT Profile Improper Access Control Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1228: Trend Micro Deep Discovery Inspector SQL Injection Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1227: Trend Micro Deep Discovery Inspector SQL Injection Information Disclosure Vulnerability

- Link

—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 X-Correlation-Id: An der Flughafen-Security vorbei mit SQL-Injection.

Zum Youtube Video

6 Cyberangriffe: (Sep)

Datum	Opfer	Land	Information
2024-09-16	TAAG	[AGO]	Link
2024-09-16	Heinrich-Böll-Gesamtschule et Rurtal-Gymnasium	[DEU]	Link
2024-09-15	Radio Geretsried	[DEU]	Link
2024-09-14	Zacros	[JPN]	Link
2024-09-12	⊠⊠⊠⊠⊠⊠ (Kantsu)	[JPN]	Link
2024-09-12	LolaLiza	[BEL]	Link
2024-09-09	Université de Gênes	[ITA]	Link
2024-09-08	Highline Public Schools	[USA]	Link
2024-09-08	Groupe Bayard	[FRA]	Link
2024-09-08	Isbergues	[FRA]	Link
2024-09-06	Superior Tribunal de Justiça (STJ)	[BRA]	Link
2024-09-05	Air-e	[COL]	Link
2024-09-05	Charles Darwin School	[GBR]	Link
2024-09-05	Elektroskandia	[SWE]	Link
2024-09-04	Tewkesbury Borough Council	[GBR]	Link
2024-09-04	Swire Pacific Offshore (SPO)	[SGP]	Link
2024-09-02	Transport for London (TfL)	[GBR]	Link
2024-09-02	Conseil national de l'ordre des experts-comptables (CNOEC)	[FRA]	Link
2024-09-02	Kawasaki Motors Europe	[GBR]	Link
2024-09-01	Wertachkliniken	[DEU]	Link

7 Ransomware-Erpressungen: (Sep)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-17	[miit.gov.cn]	killsec	Link
2024-09-17	[New Electric]	hunters	Link
2024-09-17	[AutoCanada]	hunters	Link
2024-09-17	[natcoglobal.com]	cactus	Link
2024-09-17	[Sherr Puttmann Akins Lamb PC]	bianlian	Link
2024-09-17	[peerlessumbrella.com]	cactus	Link
2024-09-17	[thomas-lloyd.com]	cactus	Link
2024-09-16	[Cruz Marine (cruz.local)]	lynx	Link
2024-09-16	[SuperCommerce.ai]	killsec	Link
2024-09-16	[MCNA Dental 1 million patients records]	everest	Link
2024-09-16	[ExcelPlast Tunisie]	orca	Link
2024-09-16	[northernsafety.com]	blackbasta	Link
2024-09-16	[thompsoncreek.com]	blackbasta	Link
2024-09-07	[www.atlcc.net]	ransomhub	Link
2024-09-10	[accuraterailroad.com]	ransomhub	Link
2024-09-10	[advantagecdc.org]	ransomhub	Link
2024-09-10	[lafuturasrl.it]	ransomhub	Link
2024-09-15	[dowley.com]	lockbit3	Link
2024-09-15	[apexbrasil.com.br]	lockbit3	Link
2024-09-15	[fivestarproducts.com]	lockbit3	Link
2024-09-15	[ignitarium.com]	lockbit3	Link
2024-09-15	[nfcaa.org]	lockbit3	Link
2024-09-15	[Emtel]	arcusmedia	Link
2024-09-15	[EAGLE School]	qilin	Link
2024-09-15	[salaam.af]	lockbit3	Link
2024-09-15	[INTERNAL.ROCKYMOUNTAINGASTRO.COM]	trinity	Link
2024-09-10	[City of Pleasanton, California]	ValenciaLeaks	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-14	[Gino Giglio Generation Spa]	arcusmedia	Link
2024-09-14	[Rextech]	arcusmedia	Link
2024-09-14	[Like Family's]	arcusmedia	Link
2024-09-14	[UNI-PA A.Ş]	arcusmedia	Link
2024-09-12	[OnePoint Patient Care]	incransom	Link
2024-09-14	[Retemex]	ransomexx	Link
2024-09-14	[ORCHID-ORTHO.COM]	clop	Link
2024-09-11	[jatelindo]	stormous	Link
2024-09-13	[mivideo.club]	stormous	Link
2024-09-12	[Micron Internet]	medusa	Link
2024-09-12	[TECHNOLOG S.r.l.]	medusa	Link
2024-09-14	[ecbawm.com]	abyss	Link
2024-09-13	[FD Lawrence Electric]	blacksuit	Link
2024-09-13	[True Family Enterprises]	play	Link
2024-09-13	[Dimensional Merchandising]	play	Link
2024-09-13	[Creative Playthings]	play	Link
2024-09-13	[Law Offices of Michael J Gurfinkel, Inc]	bianlian	Link
2024-09-13	[Hostetler Buildings]	blacksuit	Link
2024-09-13	[VIcom Corporation]	hunters	Link
2024-09-13	[Arch-Con]	hunters	Link
2024-09-13	[HB Construction]	hunters	Link
2024-09-13	[Associated Building Specialties]	hunters	Link
2024-09-12	[www.southeasternretina.com]	ransomhub	Link
2024-09-11	[Ascend Analytics (ascendanalytics.com)]	lynx	Link
2024-09-06	[Kingsmill Resort]	qilin	Link
2024-09-12	[brunswickhospitalcenter.org]	threeam	Link
2024-09-12	[Carpenter McCadden and Lane LLP]	meow	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-12	[CSMR Agrupación de Colaboración Empresaria]	meow	Link
2024-09-11	[ICBC (London)]	hunters	Link
2024-09-12	[thornton-inc.com]	ransomhub	Link
2024-09-04	[nhbg.com.co]	lockbit3	Link
2024-09-12	[mechdyne.com]	ransomhub	Link
2024-09-10	[Starr-Iva Water & Sewer District]	medusa	Link
2024-09-10	[Karakaya Group]	medusa	Link
2024-09-10	[allamericanpoly.com]	ransomhub	Link
2024-09-11	[Charles Darwin School]	blacksuit	Link
2024-09-11	[S. Walter Packaging]	fog	Link
2024-09-11	[Clatronic International GmbH]	fog	Link
2024-09-11	[Advanced Physician Management Services LLC]	meow	Link
2024-09-11	[Arville]	meow	Link
2024-09-11	[ICBC London]	hunters	Link
2024-09-11	[Ladov Law Firm]	bianlian	Link
2024-09-10	[Regent Care Center]	incransom	Link
2024-09-10	[www.vinatiorganics.com]	ransomhub	Link
2024-09-10	[Evans Distribution Systems]	play	Link
2024-09-10	[Weldco-Beales Manufacturing]	play	Link
2024-09-10	[PIGGLY WIGGLY ALABAMA DISTRIBUTING]	play	Link
2024-09-10	[Elgin Separation Solutions]	play	Link
2024-09-10	[Bel-Air Bay Club]	play	Link
2024-09-10	[Joe Swartz Electric]	play	Link
2024-09-10	[Virginia Dare Extract Co.]	play	Link
2024-09-10	[Southeast Cooler]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-10	[IDF and Mossad agents]	meow	Link
2024-09-10	[rupicard.com]	killsec	Link
2024-09-10	[Vickers Engineering]	akira	Link
2024-09-09	[Controlled Power]	dragonforce	Link
2024-09-09	[Arc-Com]	dragonforce	Link
2024-09-10	[HDI]	bianlian	Link
2024-09-10	[Myelec Electrical]	meow	Link
2024-09-10	[Kadokawa Co Jp]	blacksuit	Link
2024-09-10	[Qeco/coeq]	rhysida	Link
2024-09-10	[E-Z Pack Holdings LLC]	incransom	Link
2024-09-10	[Bank Rakyat]	hunters	Link
2024-09-06	[americagraphics.com]	ransomhub	Link
2024-09-09	[Pennsylvania State Education Association]	rhysida	Link
2024-09-09	[Anniversary Holding]	bianlian	Link
2024-09-09	[Battle Lumber Co.]	bianlian	Link
2024-09-09	[www.unige.it]	ransomhub	Link
2024-09-09	[Appellation vins fins]	ransomhub	Link
2024-09-07	[www.dpe.go.th]	ransomhub	Link
2024-09-09	[www.bsg.com.au]	ransomhub	Link
2024-09-09	[schynsassurances.be]	killsec	Link
2024-09-09	[pv.be]	killsec	Link
2024-09-09	[Smart Source, Inc.]	bianlian	Link
2024-09-08	[CAM Tyre Trade Systems & Solutions]	qilin	Link
2024-09-06	[▒▒▒▒▒▒▒▒]	cicada3301	Link
2024-09-08	[Stratford School Academy]	rhysida	Link
2024-09-07	[cardiovirginia.com]	ransomhub	Link
2024-09-07	[Prosolit]	medusa	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-07	[Grupo Cortefiel]	medusa	Link
2024-09-07	[Nocciole Marchisio]	meow	Link
2024-09-07	[Elsoms Seeds]	meow	Link
2024-09-07	[Millsboro Animal Hospital]	qilin	Link
2024-09-05	[briedis.lt]	ransomhub	Link
2024-09-06	[America Voice]	medusa	Link
2024-09-06	[CK Associates]	bianlian	Link
2024-09-06	[Keya Accounting and Tax Services LLC]	bianlian	Link
2024-09-06	[ctelift.com]	madliberator	Link
2024-09-06	[SESAM Informatics]	hunters	Link
2024-09-06	[riomarineinc.com]	cactus	Link
2024-09-06	[champeau.com]	cactus	Link
2024-09-05	[cda.be]	killsec	Link
2024-09-05	[belfius.be]	killsec	Link
2024-09-05	[dvv.be]	killsec	Link
2024-09-05	[Custom Security Systems]	hunters	Link
2024-09-05	[Inglenorth.co.uk]	ransomhub	Link
2024-09-05	[cps-k12.org]	ransomhub	Link
2024-09-05	[inorde.com]	ransomhub	Link
2024-09-05	[PhD Services]	dragonforce	Link
2024-09-05	[kawasaki.eu]	ransomhub	Link
2024-09-01	[cbt-gmbh.de]	ransomhub	Link
2024-09-05	[www.towellengineering.net]	ransomhub	Link
2024-09-04	[rhp.com.br]	lockbit3	Link
2024-09-05	[Baird Mandalas Brockstedt LLC]	akira	Link
2024-09-05	[Imetame]	akira	Link
2024-09-05	[SWISS CZ]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-05	[Cellular Plus]	akira	Link
2024-09-05	[Arch Street Capital Advisors]	qilin	Link
2024-09-04	[Hospital Episcopal San Lucas]	medusa	Link
2024-09-05	[www.parknfly.ca]	ransomhub	Link
2024-09-05	[Western Supplies, Inc]	bianlian	Link
2024-09-04	[Farmers' Rice Cooperative]	play	Link
2024-09-04	[Bakersfield]	play	Link
2024-09-04	[Crain Group]	play	Link
2024-09-04	[Parrish]	blacksuit	Link
2024-09-04	[www.galgorm.com]	ransomhub	Link
2024-09-04	[www.pcipa.com]	ransomhub	Link
2024-09-04	[ych.com]	madliberator	Link
2024-09-03	[idom.com]	lynx	Link
2024-09-04	[plannedparenthood.org]	ransomhub	Link
2024-09-04	[Sunrise Erectors]	hunters	Link
2024-09-03	[simson-maxwell.com]	cactus	Link
2024-09-03	[balboabayresort.com]	cactus	Link
2024-09-03	[flodraulic.com]	cactus	Link
2024-09-03	[mcphillips.co.uk]	cactus	Link
2024-09-03	[rangeramerican.com]	cactus	Link
2024-09-02	[Kingsport Imaging Systems]	medusa	Link
2024-09-02	[Removal.AI]	ransomhub	Link
2024-09-02	[Project Hospitality]	rhysida	Link
2024-09-02	[Shomof Group]	medusa	Link
2024-09-02	[www.sanyo-av.com]	ransomhub	Link
2024-09-01	[Quálitas México]	hunters	Link
2024-09-01	[welland]	trinity	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.