Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240926

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

Teamviewer: Hochriskante Lücken ermöglichen Rechteausweitung

In der Fernwartungssoftware Teamviewer klaffen Sicherheitslücken, durch die Angreifer ihre Rechte ausweiten können. Updates schließen sie.

- Link

—

HPE Aruba: Access Points für Codeschmuggel aus dem Netz anfällig

Hewlett Packard Enterprise (HPE) warnt vor kritischen Sicherheitslücken in Aruba Access Points. Angreifer können aus dem Netz Schadcode einschleusen.

- Link

—

Monitoring-Software checkmk: Sicherheitslücke ermöglicht 2FA-Umgehung

Eine Sicherheitslücke in der Monitoring-Software checkmk ermöglicht Angreifern, die Zwei-Faktor-Authentifizierung zu umgehen.

- Link

—

Sicherheitsupdates: Atlassian Bitbucket, Confluence & Co. attackierbar

Angreifer können an mehreren Schwachstellen in Software von Atlassian ansetzen und sie via DoS-Attacke abstürzen lassen.

- Link

—

Jetzt patchen! Attacken auf Ivanti Cloud Service Appliance verschärfen sich

Derzeit kombinieren Angreifer zwei Sicherheitslücken, um auf Cloud Services Appliances von Ivanti Schadcode auszuführen.

- Link

—

Kritische SAML-Anmelde-Lücke mit Höchstwertung gefährdet Gitlab-Server

Unter bestimmten Voraussetzungen können sich Angreifer Zugriff auf die DevSecOps-Plattform Gitlab verschaffen.

- Link

—

Sicherheitsupdates: BIOS-Lücken gefährden Dell-Computer

Unter anderem sind bestimmte Computer von Dells Alienware-Serie attackierbar. Sicherheitspatches stehen zum Download.

- Link

—

Sicherheitslücken: Netzwerk-Controller und -Gateways von Aruba sind verwundbar

Angreifer können Netzwerkgeräte von HPE Aruba attackieren und im schlimmsten Fall Appliances kompromittieren.

- Link

—

VMware vCenter: Angreifer aus dem Netz können Schadcode einschleusen

Broadcom stopft mehrere Sicherheitslücken in VMware vCenter. Schlimmstenfalls können Angreifer aus dem Netz Schadcode einschmuggeln und ausführen.

- Link

—

Samsung-Druckertreiber ermöglichen Angreifern Rechteausweitung

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

- 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	0.957580000	0.994790000	Link
CVE-2023-6895	0.927330000	0.990700000	Link
CVE-2023-6553	0.947820000	0.993110000	Link
CVE-2023-6019	0.918710000	0.989910000	Link
CVE-2023-52251	0.949200000	0.993330000	Link
CVE-2023-4966	0.970840000	0.998150000	Link
CVE-2023-49103	0.949680000	0.993430000	Link
CVE-2023-48795	0.964670000	0.996200000	Link
CVE-2023-47246	0.961220000	0.995430000	Link
CVE-2023-46805	0.957170000	0.994730000	Link
CVE-2023-46747	0.971540000	0.998420000	Link
CVE-2023-46604	0.969070000	0.997520000	Link
CVE-2023-4542	0.948590000	0.993220000	Link
CVE-2023-43208	0.974060000	0.999420000	Link
CVE-2023-43177	0.958390000	0.994920000	Link
CVE-2023-42793	0.970970000	0.998210000	Link
CVE-2023-41265	0.907590000	0.989140000	Link
CVE-2023-39143	0.940700000	0.992180000	Link
CVE-2023-38205	0.949280000	0.993340000	Link
CVE-2023-38203	0.965830000	0.996580000	Link
CVE-2023-38146	0.919150000	0.989960000	Link
CVE-2023-38035	0.974550000	0.999650000	Link
CVE-2023-36845	0.967850000	0.997150000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3519	0.965910000	0.996600000	Link
CVE-2023-35082	0.966710000	0.996820000	Link
CVE-2023-35078	0.971130000	0.998280000	Link
CVE-2023-34993	0.973450000	0.999170000	Link
CVE-2023-34960	0.900520000	0.988710000	Link
CVE-2023-34634	0.923140000	0.990310000	Link
CVE-2023-34362	0.970450000	0.997980000	Link
CVE-2023-34039	0.945100000	0.992670000	Link
CVE-2023-3368	0.942240000	0.992340000	Link
CVE-2023-33246	0.969870000	0.997770000	Link
CVE-2023-32315	0.971490000	0.998410000	Link
CVE-2023-30625	0.953820000	0.994170000	Link
CVE-2023-30013	0.965950000	0.996610000	Link
CVE-2023-29300	0.967820000	0.997140000	Link
CVE-2023-29298	0.969390000	0.997600000	Link
CVE-2023-28432	0.920500000	0.990080000	Link
CVE-2023-28343	0.937460000	0.991790000	Link
CVE-2023-28121	0.922260000	0.990240000	Link
CVE-2023-27524	0.970600000	0.998020000	Link
CVE-2023-27372	0.974150000	0.999480000	Link
CVE-2023-27350	0.969520000	0.997640000	Link
CVE-2023-26469	0.953540000	0.994100000	Link
CVE-2023-26360	0.964390000	0.996130000	Link
CVE-2023-26035	0.968720000	0.997400000	Link
CVE-2023-25717	0.950620000	0.993560000	Link
CVE-2023-25194	0.965150000	0.996390000	Link
CVE-2023-2479	0.963230000	0.995850000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-24489	0.973150000	0.999040000	Link
CVE-2023-23752	0.952050000	0.993800000	Link
CVE-2023-23333	0.960430000	0.995240000	Link
CVE-2023-22527	0.970940000	0.998190000	Link
CVE-2023-22518	0.957870000	0.994830000	Link
CVE-2023-22515	0.973160000	0.999060000	Link
CVE-2023-21839	0.947720000	0.993090000	Link
CVE-2023-21554	0.952650000	0.993950000	Link
CVE-2023-20887	0.970950000	0.998210000	Link
CVE-2023-1671	0.962220000	0.995630000	Link
CVE-2023-0669	0.971300000	0.998350000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 25 Sep 2024

[NEU] [hoch] Google Chrome: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Wed, 25 Sep 2024

[NEU] [hoch] Aruba ArubaOS: Mehrere Schwachstellen ermöglichen Ausführen von beliebigem Programmcode mit Administratorrechten

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Aruba ArubaOS ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen.

- Link

—

Wed, 25 Sep 2024

[UPDATE] [hoch] quagga: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in quagga ausnutzen um Informationen offenzulegen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen und um einen Denial of Service Zustand herbeizuführen.
- Link

—

Wed, 25 Sep 2024

[UPDATE] [hoch] expat: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in expat ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Wed, 25 Sep 2024

[UPDATE] [hoch] xpdf: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in xpdf ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

Wed, 25 Sep 2024

[UPDATE] [hoch] xpdf: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in xpdf ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

Wed, 25 Sep 2024

[UPDATE] [hoch] xpdf: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in xpdf ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

Wed, 25 Sep 2024

[UPDATE] [hoch] xpdf: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in xpdf ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

Wed, 25 Sep 2024

[UPDATE] [hoch] xpdf: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in xpdf ausnutzen, um einen Denial of

Service Angriff durchzuführen.

- Link

—

Wed, 25 Sep 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 25 Sep 2024

[UPDATE] [hoch] GNU Emacs: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in GNU Emacs ausnutzen, um beliebigen Programmcode auszuführen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 25 Sep 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

—

Wed, 25 Sep 2024

[UPDATE] [hoch] Microsoft Azure: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein Angreifer kann mehrere Schwachstellen in Microsoft Azure ausnutzen, um seine Privilegien zu erhöhen und um einen Denial of Service Zustand herbeizuführen.

- Link

—

Wed, 25 Sep 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in GNU Emacs ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 25 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

—

Wed, 25 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

—

Wed, 25 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

—

Wed, 25 Sep 2024

[UPDATE] [kritisch] FRRouting Project FRRouting: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in FRRouting Project FRRouting ausnutzen, um einen Denial of Service Zustand zu erzeugen und potenziell beliebigen Programmcode auszuführen.

- Link

—

Wed, 25 Sep 2024

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

Ein entfernter anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat OpenShift Container Platform ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen, Dateien und Daten zu manipulieren oder Sicherheitsmaßnahmen zu umgehen.

- Link

—

Wed, 25 Sep 2024

[UPDATE] [hoch] GitLab: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in GitLab und Ruby ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/25/2024	[Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-7009-2)]	critical
9/25/2024	[RHEL 7 : httpd (RHSA-2024:7101)]	critical
9/25/2024	[AlmaLinux 8 : emacs (ALSA-2024:6987)]	critical
9/25/2024	[AlmaLinux 8 : expat (ALSA-2024:6989)]	critical
9/25/2024	[AlmaLinux 8 : kernel-rt (ALSA-2024:7001)]	critical
9/25/2024	[AlmaLinux 8 : kernel (ALSA-2024:7000)]	critical
9/25/2024	[Ubuntu 20.04 LTS / 22.04 LTS : AppArmor vulnerability (USN-7035-1)]	critical
9/25/2024	[Oracle Linux 8 : kernel (ELSA-2024-7000)]	critical
9/25/2024	[SUSE SLES15 / openSUSE 15 Security Update : python39 (SUSE-SU-2024:3411-1)]	high
9/25/2024	[SUSE SLES15 Security Update : kernel (SUSE-SU-2024:3408-1)]	high
9/25/2024	[SUSE SLES15 Security Update : kernel (Live Patch 18 for SLE 15 SP4) (SUSE-SU-2024:3425-1)]	high
9/25/2024	[SUSE SLES12 Security Update : python36 (SUSE-SU-2024:3430-1)]	high
9/25/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : python311 (SUSE-SU-2024:3418-1)]	high
9/25/2024	[FreeBSD : frr - BGP (802961eb-7a89-11ef-bdd7-a0423f48a938)]	high
9/25/2024	[ArubaOS 8.10.x < 8.10.0.14, 8.12.x < 8.12.0.2, 10.6.x < 10.6.0.3 Multiple Vulnerabilities (HPESBNW04709)]	high
9/25/2024	[RHEL 9 : grafana (RHSA-2024:7102)]	high
9/25/2024	[RHEL 9 : grafana-pcp (RHSA-2024:7103)]	high

Datum	Schwachstelle	Bewertung
9/25/2024	[AlmaLinux 8 : go-toolset:rhel8 (ALSA-2024:6908)]	high
9/25/2024	[AlmaLinux 8 : gtk3 (ALSA-2024:6963)]	high
9/25/2024	[AlmaLinux 8 : python3.12 (ALSA-2024:6961)]	high
9/25/2024	[AlmaLinux 8 : python3.11 (ALSA-2024:6962)]	high
9/25/2024	[AlmaLinux 9 : grafana (ALSA-2024:6947)]	high
9/25/2024	[AlmaLinux 9 : golang (ALSA-2024:6913)]	high
9/25/2024	[AlmaLinux 8 : container-tools:rhel8 (ALSA-2024:6969)]	high
9/25/2024	[AlmaLinux 9 : grafana-pcp (ALSA-2024:6946)]	high
9/25/2024	[AlmaLinux 8 : virt:rhel and virt-devel:rhel (ALSA-2024:6964)]	high
9/25/2024	[AlmaLinux 8 : python3 (ALSA-2024:6975)]	high
9/25/2024	[CBL Mariner 2.0 Security Update: gdk-pixbuf2 (CVE-2022-48622)]	high
9/25/2024	[CBL Mariner 2.0 Security Update: ruby / rubygem-rexml (CVE-2024-41946)]	high
9/25/2024	[Debian dla-3895 : puredata - security update]	high
9/25/2024	[RHEL 9 : git-lfs (RHSA-2024:7136)]	high
9/25/2024	[RHEL 8 : git-lfs (RHSA-2024:7135)]	high
9/25/2024	[Oracle Linux 8 : python3.11 (ELSA-2024-6962)]	high
9/25/2024	[Oracle Linux 8 : python3.12 (ELSA-2024-6961)]	high
9/25/2024	[Oracle Linux 8 : virt:ol / and / virt-devel:rhel (ELSA-2024-6964)]	high
9/25/2024	[Oracle Linux 8 : container-tools:ol8 (ELSA-2024-6969)]	high
9/25/2024	[Siemens (CVE-2024-34057)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Wed, 25 Sep 2024

ABB Cylon Aspect 3.07.00 Remote Code Execution

The ABB Cylon Aspect version 3.07.00 BMS/BAS controller suffers from an unauthenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the host HTTP GET parameter called by networkDiagAjax.php script.

- Link

—

” “Wed, 25 Sep 2024

PHP SPM 1.0 Code Injection

PHP SPM version 1.0 suffers from a PHP code injection vulnerability.

- Link

—

” “Wed, 25 Sep 2024

PHP ACRSS 1.0 Code Injection

PHP ACRSS version 1.0 suffers from a PHP code injection vulnerability.

- Link

—

” “Wed, 25 Sep 2024

Online mcq System 1.0 Cross Site Scripting

Online mcq System version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Wed, 25 Sep 2024

Online Job Search System 1.0 Arbitrary File Upload

Online Job Search System version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Wed, 25 Sep 2024

Online Flight Booking System 1.0 Arbitrary File Upload

Online Flight Booking System version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Wed, 25 Sep 2024

Multi Branch School Management System 3.5 Backup Disclosure

Multi Branch School Management System version 3.5 suffers from a backup disclosure vulnerability.
- Link

—

” “Wed, 25 Sep 2024

Complete Multi Hospital Management System 1.0 Backup Disclosure

Complete Multi Hospital Management System version 1.0 suffers from a backup disclosure vulnerability.
- Link

—

” “Wed, 25 Sep 2024

Traccar 5.1 Code Injection

Traccar version 5.1 suffers from a PHP code injection vulnerability.
- Link

—

” “Tue, 24 Sep 2024

ABB Cylon Aspect 3.08.01 Remote Code Execution

ABB Cylon Aspect version 3.08.01 BMS/BAS controller suffers from a remote code execution vulnerability. The vulnerable uploadFile() function in bigUpload.php improperly reads raw POST data using the php://input wrapper without sufficient validation. This data is passed to the fwrite() function, allowing arbitrary file writes. Combined with an improper sanitization of file paths, this leads to directory traversal, allowing an attacker to upload malicious files to arbitrary locations. Once a malicious file is written to an executable directory, an authenticated attacker can trigger the file to execute code and gain unauthorized access to the building controller.
- Link

—

” “Tue, 24 Sep 2024

ABB Cylon Aspect 3.08.01 Arbitrary File Deletion

ABB Cylon Aspect version 3.08.01 MS/BAS controller suffers from an arbitrary file deletion vulnerability. Input passed to the file parameter in databasefiledelete.php is not properly sanitized before being used to delete files. This can be exploited by an unauthenticated attacker to delete files with the permissions of the web server using directory traversal sequences passed within the affected POST parameter.
- Link

—

” “Tue, 24 Sep 2024

Traccar 5.12 Remote Code Execution

This Metasploit module exploits a remote code execution vulnerability in Traccar versions 5.1 through 5.12. Remote code execution can be obtained by combining path traversal and an unrestricted file

upload vulnerabilities. By default, the application allows self-registration, enabling any user to register an account and exploit the issues. Moreover, the application runs by default with root privileges, potentially resulting in a complete system compromise. This Metasploit module, which should work on any Red Hat-based Linux system, exploits these issues by adding a new cronjob file that executes the specified payload.

- Link

—

” “Tue, 24 Sep 2024

Apple iOS 17.2.1 Screen Time Passcode Retrieval / Mitigation Bypass

A mitigation bypass / privilege escalation flaw has been discovered in Apple’s iOS Screen Time functionality, granting one access to modify the restrictions. It allows a local attacker to acquire the Screen Time Passcode by bypassing the anti-bruteforce protections on the four-digit Passcode, and in consequence gaining total control over Screen Time (Parental Control) settings. Versions lower than 18 are affected.

- Link

—

” “Tue, 24 Sep 2024

Netman 204 4.05 SQL Injection / Unauthenticated Password Reset

Netman 204 version 4.05 suffers from remote SQL injection and unauthenticated password reset vulnerabilities.

- Link

—

” “Tue, 24 Sep 2024

Elaine’s Realtime CRM Automation 6.18.17 Cross Site Scripting

Elaine’s Realtime CRM Automation version 6.18.17 suffers from a cross site scripting vulnerability.

- Link

—

” “Tue, 24 Sep 2024

PHP ACRSS 1.0 Cross Site Request Forgery

PHP ACRSS version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Tue, 24 Sep 2024

Reservation Management System 1.0 Backup Disclosure

Reservation Management System version 1.0 suffers from a backup disclosure vulnerability.

- Link

—

” “Tue, 24 Sep 2024

Rail Pass Management System 1.0 Insecure Settings

Rail Pass Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Tue, 24 Sep 2024

PreSchool Enrollment System 1.0 Insecure Settings

PreSchool Enrollment System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Tue, 24 Sep 2024

PHP SPM 1.0 Cross Site Request Forgery

PHP SPM version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Tue, 24 Sep 2024

Online MCQ System 1.0 SQL Injection

Online MCQ System version 1.0 suffers from a remote blind SQL injection vulnerability.

- Link

—

” “Tue, 24 Sep 2024

Online Flight Booking System 1.0 Cross Site Request Forgery

Online Flight Booking System version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Tue, 24 Sep 2024

Lost And Found Information System 1.0 WYSIWYG Code Injection

Lost and Found Information System version 1.0 suffers from a WYSIWYG code injection vulnerability.

- Link

—

” “Tue, 24 Sep 2024

Car Rental Project 1.0 Code Injection

Car Rental Project version 1.0 suffers from a remote PHP code injection vulnerability.

- Link

—

” “Tue, 24 Sep 2024

Blood Pressure Monitoring System 1.0 SQL Injection

Blood Pressure Monitoring System version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—
”

4.2 0-Days der letzten 5 Tage

“Wed, 25 Sep 2024
ZDI-24-1288: Apple macOS AppleIntelKBLGraphicsMTLDriver Out-Of-Bounds Write Remote Code Execution Vulnerability
- Link
—
” “Wed, 25 Sep 2024
ZDI-24-1287: Apple macOS AppleVADriver Out-Of-Bounds Write Remote Code Execution Vulnerability
- Link
—
” “Wed, 25 Sep 2024
ZDI-24-1286: Apple macOS AppleGVA Out-Of-Bounds Read Information Disclosure Vulnerability
- Link
—
” “Wed, 25 Sep 2024
ZDI-24-1285: Apple macOS VideoToolbox Uninitialized Memory Information Disclosure Vulnerability
- Link
—
” “Wed, 25 Sep 2024
ZDI-24-1284: Apple macOS AppleIntelKBLGraphicsMTLDriver Out-Of-Bounds Read Remote Code Execution Vulnerability
- Link
—
” “Wed, 25 Sep 2024
ZDI-24-1283: Apple macOS ImageIO JP2 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability
- Link
—
” “Wed, 25 Sep 2024
ZDI-24-1282: Apple macOS AppleGVA Out-Of-Bounds Read Information Disclosure Vulnerability
- Link
—

” “Wed, 25 Sep 2024

ZDI-24-1281: Apple macOS AppleVADriver Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Wed, 25 Sep 2024

ZDI-24-1280: Apple macOS AppleVADriver Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Wed, 25 Sep 2024

ZDI-24-1279: Apple macOS AppleVADriver Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Wed, 25 Sep 2024

ZDI-24-1278: Apple macOS AppleVADriver Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Wed, 25 Sep 2024

ZDI-24-1277: Apple macOS AppleVADriver Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Wed, 25 Sep 2024

ZDI-24-1276: Apple macOS AppleVADriver Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Mon, 23 Sep 2024

ZDI-24-1275: (0Day) FastStone Image Viewer GIF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Mon, 23 Sep 2024

ZDI-24-1274: (0Day) FastStone Image Viewer TGA File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Mon, 23 Sep 2024

ZDI-24-1273: (0Day) FastStone Image Viewer PSD File Parsing Out-Of-Bounds Write Remote Code Execution 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
2024-09-23	VBG Unfallversicherung	[DEU]	Link
2024-09-22	Schumag Aktiengesellschaft	[DEU]	Link
2024-09-22	Arkansas City Water Plant	[USA]	Link
2024-09-22	MoneyGram	[USA]	Link
2024-09-21	Namebay	[MCO]	Link
2024-09-20	Delaware libraries	[USA]	Link
2024-09-19	Fernando Prestes	[BRA]	Link
2024-09-16	TAAG	[AGO]	Link
2024-09-16	Heinrich-Böll-Gesamtschule et Rurtal-Gymnasium	[DEU]	Link
2024-09-16	Fylde Coast Academy Trust	[GBR]	Link
2024-09-15	Radio Geretsried	[DEU]	Link
2024-09-15	Technet	[NOR]	Link
2024-09-14	Zacros	[JPN]	Link
2024-09-12	⊠⊠⊠⊠⊠⊠ (Kantsu)	[JPN]	Link
2024-09-12	LolaLiza	[BEL]	Link
2024-09-11	Providence Public School District (PPSD)	[USA]	Link
2024-09-11	Town of Ulster	[USA]	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

Datum	Opfer	Land	Information
2024-09-04	Tewkesbury Borough Council	[GBR]	Link
2024-09-04	Swire Pacific Offshore (SPO)	[SGP]	Link
2024-09-04	Compass Group	[AUS]	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
2024-09-23	[DETROIT PBS (PUBLIC TV)]	qilin	Link
2024-09-25	[Concord Management Services]	akira	Link
2024-09-25	[Lawrie Insurance Group]	akira	Link
2024-09-25	[ATG Communications Group]	akira	Link
2024-09-25	[Luso Cuanza]	qilin	Link
2024-09-23	[Hairstore]	medusa	Link
2024-09-23	[IP blue Software Solutions]	medusa	Link
2024-09-25	[Pennvet.com]	cloak	Link
2024-09-25	[triverus.com]	lynx	Link
2024-09-25	[hindlegroup.com]	cactus	Link
2024-09-25	[kjtait.com]	cactus	Link
2024-09-25	[www.amchar.com]	cactus	Link
2024-09-24	[libraries.delaware.gov]	ransomhub	Link
2024-09-24	[gsdwi.org]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-24	[PetEdge]	play	Link
2024-09-15	[Bogdan Frasco, LLP]	cicada3301	Link
2024-09-15	[John W. Brooker Co., CPAs]	cicada3301	Link
2024-09-24	[Hughes Gill Cochrane Tinetti]	cicada3301	Link
2024-09-24	[Menninger Clinic]	blacksuit	Link
2024-09-24	[Israel defense minister private photos]	handala	Link
2024-09-24	[cottlesinc.com]	blacksuit	Link
2024-09-24	[Crown Mortgage Company]	cicada3301	Link
2024-09-24	[First Choice Sales & Marketing Group (First Choice)]	bianlian	Link
2024-09-24	[Frigocenter]	arcusmedia	Link
2024-09-24	[Partners Air]	arcusmedia	Link
2024-09-24	[Solutii Sistemas]	arcusmedia	Link
2024-09-24	[Nova Sinseg]	arcusmedia	Link
2024-09-23	[Model Engineering]	cicada3301	Link
2024-09-14	[tellurianinc.org]	ransomhub	Link
2024-09-23	[Kravit, Hovel & Krawczyk SC]	qilin	Link
2024-09-23	[BroadGrain Commodities]	play	Link
2024-09-23	[Eurobulk]	play	Link
2024-09-23	[www.datacampos.com]	ElDorado	Link
2024-09-23	[cucinatagliani.com]	ElDorado	Link
2024-09-23	[cmclb.com]	ElDorado	Link
2024-09-23	[f-t.com]	abyss	Link
2024-09-23	[oleopalma.com.mx]	lockbit3	Link
2024-09-23	[Avi Resort & Casino]	akira	Link
2024-09-23	[DIamond Contracting, LLC]	qilin	Link
2024-09-23	[medicheck.io]	killsec	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-23	[Benny Gantz]	handala	Link
2024-09-23	[Brown Bottling Group]	akira	Link
2024-09-23	[bakpilic.com.tr]	ransomhub	Link
2024-09-23	[Pureform Radiology Center]	everest	Link
2024-09-23	[Idre Fjäll]	akira	Link
2024-09-23	[Detroit Public TV]	qilin	Link
2024-09-23	[ten8fire.com]	cactus	Link
2024-09-23	[Fabrica Industrial Machinery & Equipment]	trinity	Link
2024-09-23	[Graminex]	dragonforce	Link
2024-09-23	[Canstar Restorations]	qilin	Link
2024-09-22	[hanwa.co.th]	BrainCipher	Link
2024-09-22	[Daughterly Care]	rhysida	Link
2024-09-22	[Woodard , Hernandez , Roth & Day]	qilin	Link
2024-09-20	[savannahcandy.com]	ransomhub	Link
2024-09-21	[Acho.io]	ransomhub	Link
2024-09-05	[Bayou DeSiard Country Club]	cicada3301	Link
2024-09-20	[Jackson Paper Manufacturing]	play	Link
2024-09-20	[Messe C]	play	Link
2024-09-20	[Noble Environmental]	play	Link
2024-09-20	[Omega Industries]	play	Link
2024-09-20	[Pacific Coast Building Products]	play	Link
2024-09-20	[Thompson Construction Supply]	play	Link
2024-09-20	[Visionary Homes]	incransom	Link
2024-09-20	[KW Realty Group]	qilin	Link
2024-09-20	[Capital Printing]	cicada3301	Link
2024-09-18	[virainsight.com]	ransomhub	Link
2024-09-20	[Juice Generation]	fog	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-20	[River Region Cardiology Associates]	bianlian	Link
2024-09-20	[Greene Acres Nursing Home]	rhysida	Link
2024-09-20	[aroma.com.tr]	ransomhub	Link
2024-09-19	[rarholding.com]	ransomhub	Link
2024-09-19	[Fritzøe Engros]	medusa	Link
2024-09-19	[Wilson & Lafleur]	medusa	Link
2024-09-19	[Wertachkliniken.de]	cloak	Link
2024-09-19	[newriverelectrical.com]	ElDorado	Link
2024-09-19	[seaglesafety.com]	ElDorado	Link
2024-09-19	[rccauto.com]	ElDorado	Link
2024-09-19	[itasnatta.edu.it]	ElDorado	Link
2024-09-19	[a1mobilelock.com]	ElDorado	Link
2024-09-19	[curvc.com]	ElDorado	Link
2024-09-19	[patricksanderscompany.com]	ElDorado	Link
2024-09-19	[thinksimple.com]	ElDorado	Link
2024-09-19	[pesprograms.com]	ElDorado	Link
2024-09-19	[palmfs.com]	ElDorado	Link
2024-09-19	[kennedyfunding.com]	ElDorado	Link
2024-09-19	[advbe.com]	ransomhub	Link
2024-09-19	[Sunrise Farms]	fog	Link
2024-09-19	[Nusser Mineralöl GmbH]	incransom	Link
2024-09-19	[avl1.com]	ransomhub	Link
2024-09-19	[libertyfirstcu.com]	ransomhub	Link
2024-09-19	[Hunter Dickinson Inc.]	bianlian	Link
2024-09-19	[tims.com]	abyss	Link
2024-09-18	[bspcr.com]	lockbit3	Link
2024-09-18	[lakelandchamber.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-18	[yesmoke.eu]	lockbit3	Link
2024-09-18	[efile.com]	lockbit3	Link
2024-09-18	[paybito.com]	lockbit3	Link
2024-09-18	[Compass Group (2nd attack)]	medusa	Link
2024-09-18	[Structural Concepts]	medusa	Link
2024-09-19	[Vidisco]	handala	Link
2024-09-19	[IIB (Israeli Industrial Batteries)]	handala	Link
2024-09-18	[Plaisted Companies]	play	Link
2024-09-11	[Bertelkamp Automation]	qilin	Link
2024-09-18	[DJH Jugendherberge]	hunters	Link
2024-09-18	[Prentke Romich Company]	fog	Link
2024-09-12	[agricola]	qilin	Link
2024-09-16	[Amerinational Community Services]	medusa	Link
2024-09-16	[Providence Public School Department]	medusa	Link
2024-09-16	[AZPIRED]	medusa	Link
2024-09-17	[Compass Group]	medusa	Link
2024-09-18	[Chernan Technology]	orca	Link
2024-09-18	[Port of Seattle/Seattle-Tacoma International Airport (SEA)]	rhysida	Link
2024-09-16	[Baskervill]	play	Link
2024-09-16	[Protective Industrial Products]	play	Link
2024-09-16	[Inktel]	play	Link
2024-09-16	[Rsp]	play	Link
2024-09-16	[Hariri Pontarini Architects]	play	Link
2024-09-16	[Multidata]	play	Link
2024-09-18	[Environmental Code Consultants Inc]	meow	Link
2024-09-18	[EnviroNET Inc]	meow	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-18	[Robson Planning Group Inc]	meow	Link
2024-09-16	[oipip.gda.pl]	ransomhub	Link
2024-09-16	[kryptonresources.com]	ransomhub	Link
2024-09-16	[www.tta.cls]	ransomhub	Link
2024-09-18	[globe.com.bd]	ValenciaLeaks	Link
2024-09-18	[satiagroup.com]	ValenciaLeaks	Link
2024-09-18	[duopharmabiotech.com]	ValenciaLeaks	Link
2024-09-18	[tendam.es]	ValenciaLeaks	Link
2024-09-18	[cityofpleasantonca.gov]	ValenciaLeaks	Link
2024-09-16	[www.faithfc.org]	ransomhub	Link
2024-09-16	[www.adantia.es]	ransomhub	Link
2024-09-16	[topdoctors.com]	ransomhub	Link
2024-09-16	[www.8010urbanliving.com]	ransomhub	Link
2024-09-16	[www.taperuvicha.com]	ransomhub	Link
2024-09-17	[www.plumbersstock.com]	ransomhub	Link
2024-09-17	[www.nikpol.com.au]	ransomhub	Link
2024-09-18	[www.galloway-macleod.co.uk]	ransomhub	Link
2024-09-18	[ringpower.com]	ransomhub	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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	[salaam.af]	lockbit3	Link
2024-09-15	[INTERNAL.ROCKYMOUNTAINGASTRO.COM]	trinity	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-09-12	[brunswickhospitalcenter.org]	threeam	Link
2024-09-12	[Carpenter McCadden and Lane LLP]	meow	Link
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
2024-09-11	[Charles Darwin School]	blacksuit	Link
2024-09-11	[S. Walter Packaging]	fog	Link
2024-09-11	[Clatronic International GmbH]	fog	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-09-07	[www.dpe.go.th]	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	[Prosolit]	medusa	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-09-04	[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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.