Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241027

Inhaltsverzeichnis

1 Editorial **2**

2 Security-News **3**
2.1 Heise - Security-Alert . . . 3

3 Sicherheitslücken **4**
3.1 EPSS . . . 4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit . . . 5
3.2 BSI - Warn- und Informationsdienst (WID) . . . 7
3.3 Sicherheitslücken Meldungen von Tenable . . . 11

4 Aktiv ausgenutzte Sicherheitslücken **12**
4.1 Exploits der letzten 5 Tage . . . 12
4.2 0-Days der letzten 5 Tage . . . 17

5 Die Hacks der Woche **18**
5.0.1 AI Girlfriends HACKED (Da steht uns noch was bevor) . . . 18

6 Cyberangriffe: (Okt) **19**

7 Ransomware-Erpressungen: (Okt) **20**

8 Quellen **36**
8.1 Quellenverzeichnis . . . 36

9 Impressum **38**

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

Cisco meldet mehr als 35 Sicherheitslücken in Firewall-Produkten

Ciscos ASA, Firepower und Secure Firewall Management Center weisen teils kritische Sicherheitslücken auf. Mehr als 35 schließen nun verfügbare Updates.

- Link

—

Angreifer missbrauchen Sharepoint-Sicherheitsleck für Codeschmuggel

Die IT-Sicherheitsbehörde CISA warnt vor aktuellen Angriffen auf eine Sharepoint-Schwachstelle. Sie ermöglicht Codeschmuggel.

- Link

—

Fortinet bestätigt kritische angegriffene Sicherheitslücke in Fortimanager

Fortinet hat eine kritische Sicherheitslücke in Fortimanager bestätigt, die bereits angegriffen wird. Updates stehen seit Kurzem bereit.

- Link

—

Sicherheitslücke in Samsung-Android-Treiber wird angegriffen

Treiber für Samsungs Mobilprozessoren ermöglichen Angreifern das Ausweiten ihrer Rechte. Google warnt vor laufenden Angriffen darauf.

- Link

—

VMware vCenter: Patch unwirksam, neues Update nötig

Mitte September hat Broadcom eine kritische Sicherheitslücke in VMware vCenter gestopft. Allerdings nicht richtig. Ein neues Update korrigiert das.

- Link

—

FortiManager: Update dichtet offenbar attackiertes Sicherheitsleck ab

Ohne öffentliche Informationen hat Fortinet Updates für FortiManager veröffentlicht. Sie schließen offenbar attackierte Sicherheitslücken.

- Link

—

Roundcube Webmail: Angriffe mit gefälschten Anhängen

IT-Sicherheitsforscher haben Angriffe auf eine Stored-Cross-Site-Scripting-Lücke in Roundcube Webmail beobachtet. Ein Update ist verfügbar.

- Link

—

Sicherheitsupdates: DoS-Attacken auf IBM-Software möglich

IBMs Entwickler haben Schwachstellen in App Connect Enterprise und WebSphere Application Server geschlossen.

- Link

—

Atlassian: Schwachstellen machen Bitbucket, Confluence und Jira verwundbar

In Bitbucket, Confluence und Jira lauern Sicherheitslücken, die etwa Informationsabfluss oder Denial-of-Service ermöglichen.

- Link

—

Ubiquiti Unifi Network Server: Hochriskantes Leck ermöglicht Rechteausweitung

In Ubiquitis Unifi Network Server klafft eine hochriskante Schwachstelle. Angreifer können dadurch ihre Rechte ausweiten.

- 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	0.994950000	Link
CVE-2023-6895	0.925010000	0.990810000	Link
CVE-2023-6553	0.945310000	0.993010000	Link
CVE-2023-6019	0.933700000	0.991650000	Link
CVE-2023-6018	0.911590000	0.989740000	Link
CVE-2023-52251	0.948240000	0.993430000	Link
CVE-2023-4966	0.971220000	0.998370000	Link
CVE-2023-49103	0.949290000	0.993580000	Link
CVE-2023-48795	0.962520000	0.995790000	Link
CVE-2023-47246	0.960640000	0.995450000	Link
CVE-2023-46805	0.962030000	0.995710000	Link
CVE-2023-46747	0.972980000	0.998990000	Link
CVE-2023-46604	0.970640000	0.998140000	Link
CVE-2023-4542	0.941060000	0.992490000	Link
CVE-2023-43208	0.974590000	0.999690000	Link
CVE-2023-43177	0.954040000	0.994360000	Link
CVE-2023-42793	0.970480000	0.998090000	Link
CVE-2023-41892	0.905460000	0.989290000	Link
CVE-2023-41265	0.920970000	0.990400000	Link
CVE-2023-38205	0.954790000	0.994450000	Link
CVE-2023-38203	0.964750000	0.996320000	Link
CVE-2023-38146	0.920950000	0.990400000	Link
CVE-2023-38035	0.974710000	0.999750000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.967260000	0.997040000	Link
CVE-2023-3519	0.965540000	0.996590000	Link
CVE-2023-35082	0.965310000	0.996530000	Link
CVE-2023-35078	0.967840000	0.997220000	Link
CVE-2023-34993	0.973050000	0.999030000	Link
CVE-2023-34634	0.923140000	0.990600000	Link
CVE-2023-34362	0.970450000	0.998070000	Link
CVE-2023-34039	0.944770000	0.992950000	Link
CVE-2023-3368	0.937940000	0.992120000	Link
CVE-2023-33246	0.971590000	0.998470000	Link
CVE-2023-32315	0.973480000	0.999180000	Link
CVE-2023-30625	0.953820000	0.994320000	Link
CVE-2023-30013	0.962230000	0.995730000	Link
CVE-2023-29300	0.967820000	0.997220000	Link
CVE-2023-29298	0.969430000	0.997690000	Link
CVE-2023-28432	0.921730000	0.990480000	Link
CVE-2023-28343	0.957970000	0.995010000	Link
CVE-2023-28121	0.929610000	0.991240000	Link
CVE-2023-27524	0.969670000	0.997780000	Link
CVE-2023-27372	0.973760000	0.999300000	Link
CVE-2023-27350	0.968980000	0.997540000	Link
CVE-2023-26469	0.955890000	0.994660000	Link
CVE-2023-26360	0.963280000	0.995960000	Link
CVE-2023-26035	0.967750000	0.997190000	Link
CVE-2023-25717	0.950620000	0.993750000	Link
CVE-2023-25194	0.966130000	0.996730000	Link
CVE-2023-2479	0.961940000	0.995690000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-24489	0.972860000	0.998940000	Link
CVE-2023-23752	0.949000000	0.993520000	Link
CVE-2023-23333	0.963480000	0.996010000	Link
CVE-2023-22527	0.970410000	0.998050000	Link
CVE-2023-22518	0.965000000	0.996400000	Link
CVE-2023-22515	0.973250000	0.999110000	Link
CVE-2023-21839	0.941470000	0.992540000	Link
CVE-2023-21554	0.952650000	0.994150000	Link
CVE-2023-20887	0.971130000	0.998330000	Link
CVE-2023-1698	0.916400000	0.990030000	Link
CVE-2023-1671	0.962340000	0.995770000	Link
CVE-2023-0669	0.971830000	0.998540000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 25 Oct 2024

[UPDATE] [hoch] EDK2 NetworkPkg IP stack implementation: Mehrere Schwachstellen

Ein Angreifer aus dem angrenzenden Netzwerk oder ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der EDK2 NetworkPkg IP stack implementation ausnutzen, um beliebigen Programmcode auszuführen, vertrauliche Informationen offenzulegen und einen Denial of Service Zustand auszulösen.

- Link

—

Fri, 25 Oct 2024

[NEU] [hoch] Rancher: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Rancher ausnutzen, um Informationen offenzulegen, erhöhte Rechte zu erlangen und beliebigen Code auszuführen.

- Link

—

Fri, 25 Oct 2024

[UPDATE] [hoch] IBM QRadar SIEM: Mehrere Schwachstellen

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

- Link

—

Fri, 25 Oct 2024

[UPDATE] [hoch] Red Hat Ansible Automation Platform: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat Ansible Automation Platform ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand erzeugen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder Cross-Site-Scripting (XSS)-Angriffe durchzuführen.

- Link

—

Fri, 25 Oct 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im RADIUS Protokoll ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Fri, 25 Oct 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

—

Fri, 25 Oct 2024

[UPDATE] [hoch] Red Hat Enterprise Linux (python-setuptools): Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 25 Oct 2024

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

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

- Link

—

Fri, 25 Oct 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

—

Fri, 25 Oct 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Thunderbird ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmaßnahmen zu umgehen, Daten zu manipulieren, einen Denial-of-Service-Zustand zu erzeugen und vertrauliche Informationen preiszugeben.

- Link

—

Fri, 25 Oct 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in CUPS cups-browsed ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Fri, 25 Oct 2024

[UPDATE] [hoch] Mozilla Firefox, Firefox ESR und Thunderbird: Schwachstelle ermöglicht Code-ausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Mozilla Firefox, Firefox ESR und Thunderbird ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 25 Oct 2024

[UPDATE] [hoch] Nvidia Treiber: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Nvidia Treibern ausnutzen, um seine Rechte zu erweitern, Code auszuführen, Daten offenzulegen oder zu manipulieren oder einen Denial of Service zu verursachen.

- Link

—

Thu, 24 Oct 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

—

Thu, 24 Oct 2024

[NEU] [hoch] Mehrere Cisco Produkte / Snort: Mehrere Schwachstelle

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Snort und Cisco Firepower ausnutzen, um Sicherheitsmaßnahmen zu umgehen und einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Thu, 24 Oct 2024

[NEU] [hoch] Drupal: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Drupal ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen, beliebigen Code auszuführen und nicht spezifizierte Auswirkungen zu verursachen.

- Link

—

Thu, 24 Oct 2024

[NEU] [hoch] Cisco Secure Firewall Management Center: Mehrere Schwachstellen

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Cisco Secure Firewall Management Center ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen, vertrauliche Informationen preiszugeben, beliebigen Code auszuführen, Daten zu manipulieren und erhöhte Rechte zu erlangen.

- Link

—

Thu, 24 Oct 2024

[NEU] [hoch] Cisco Firepower: Mehrere Schwachstellen

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Cisco Firepower ausnutzen, um Sicherheitsvorkehrungen zu umgehen, erhöhte Rechte zu erlangen und einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Thu, 24 Oct 2024

[NEU] [hoch] GitLab: Mehrere Schwachstellen ermöglichen Denial of Service und Cross-Site

Scripting

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um einen Denial of Service Angriff und einen Cross-Site-Scripting-Angriff durchzuführen.

- Link

—

Thu, 24 Oct 2024

[NEU] [hoch] Cisco Firepower und ASA: Mehrere Schwachstellen

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Cisco Firepower und Cisco ASA (Adaptive Security Appliance) ausnutzen, um Sicherheitsvorkehrungen zu umgehen, einen Denial-of-Service-Zustand zu erzeugen, beliebigen Code auszuführen, erhöhte Rechte zu erlangen und einen Cross-Site-Scripting-Angriff durchzuführen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
10/26/2024	[Fortinet Fortigate (FG-IR-23-328)]	critical
10/26/2024	[Fortinet FortiWeb (FG-IR-21-119)]	critical
10/26/2024	[Fortinet FortiWeb (FG-IR-21-130)]	critical
10/26/2024	[Fortinet Fortigate (FG-IR-21-049)]	critical
10/26/2024	[Fortinet FortiWeb sqli (FG-IR-20-124)]	critical
10/26/2024	[Fortinet FortiWeb (FG-IR-20-125)]	critical
10/27/2024	[Fortinet FortiWeb (FG-IR-21-046)]	high
10/27/2024	[Fortinet Fortigate (FG-IR-21-046)]	high
10/26/2024	[Fortinet Fortigate (FG-IR-22-073)]	high
10/26/2024	[Fortinet FortiWeb (FG-IR-23-068)]	high
10/26/2024	[Fortinet Fortigate (FG-IR-21-018)]	high
10/26/2024	[Fortinet FortiWeb (FG-IR-20-206)]	high

Datum	Schwachstelle	Bewertung
10/26/2024	[Fortinet Fortigate (FG-IR-21-201)]	high
10/26/2024	[Fortinet FortiWeb (FG-IR-21-120)]	high
10/26/2024	[Fortinet FortiWeb (FG-IR-21-131)]	high
10/26/2024	[Fortinet FortiWeb (FG-IR-21-188)]	high
10/26/2024	[Fortinet FortiWeb (FG-IR-21-152)]	high
10/26/2024	[Fortinet Fortigate (FG-IR-21-051)]	high
10/26/2024	[Fortinet Fortigate (FG-IR-21-181)]	high
10/26/2024	[Fortinet Fortigate (FG-IR-20-131)]	high
10/26/2024	[Fortinet Fortigate (FG-IR-21-235)]	high
10/26/2024	[Fortinet Fortigate (FG-IR-22-074)]	high
10/26/2024	[Fortinet FortiWeb (FG-IR-21-134)]	high
10/26/2024	[Fortinet FortiClient (FG-IR-20-040)]	high
10/26/2024	[Fortinet Fortigate (FG-IR-20-172)]	high
10/26/2024	[Fortinet Fortigate (FG-IR-23-090)]	high
10/26/2024	[Fortinet FortiWeb (FG-IR-21-116)]	high
10/25/2024	[RockyLinux 9 : kernel (RLSA-2024:8162)]	high
10/25/2024	[F5 Networks BIG-IP : Python tarfile vulnerability (K000148252)]	high
10/25/2024	[Fortinet FortiWeb (FG-IR-24-258)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Fri, 25 Oct 2024

Lawo AG vsm LTC Time Sync Path Traversal

Lawo AG vsm LTC Time Sync versions prior to 4.5.6.0 suffer from a path traversal vulnerability.

- Link

—

” “Thu, 24 Oct 2024

ABB Cylon Aspect 3.08.02 logYumLookup.php Authenticated File Disclosure

ABB Cylon Aspect version 3.08.02 suffers from an authenticated arbitrary file disclosure vulnerability. Input passed through the logFile GET parameter via the logYumLookup.php script is not properly verified before being used to download log files. This can be exploited to disclose the contents of arbitrary and sensitive files via directory traversal attacks.

- Link

—

” “Thu, 24 Oct 2024

Vendure Arbitrary File Read / Denial Of Service

Vendure is an open-source headless commerce platform. Prior to versions 3.0.5 and 2.3.3, a vulnerability in Vendure’s asset server plugin allows an attacker to craft a request which is able to traverse the server file system and retrieve the contents of arbitrary files, including sensitive data such as configuration files, environment variables, and other critical data stored on the server. In the same code path is an additional vector for crashing the server via a malformed URI. Patches are available in versions 3.0.5 and 2.3.3. Some workarounds are also available. One may use object storage rather than the local file system, e.g. MinIO or S3, or define middleware which detects and blocks requests with urls containing /../.

- Link

—

” “Thu, 24 Oct 2024

Helakuru 1.1 DLL Hijacking

Helakuru version 1.1 suffers from a dll hijacking vulnerability.

- Link

—

” “Thu, 24 Oct 2024

Grafana Remote Code Execution

This repository contains a Python script that exploits a remote code execution vulnerability in Grafana’s SQL Expressions feature. By leveraging insufficient input sanitization, this exploit allows an attacker to execute arbitrary shell commands on the server. This is made possible through the shellfs community extension, which can be installed and loaded by an attacker to facilitate command execution.

- Link

—

” “Thu, 24 Oct 2024

Roundcube Webmail Cross Site Scripting

Roundcube Webmail versions prior to 1.5.7 and 1.6.x prior to 1.6.7 allows cross site scripting via SVG animate attributes.

- Link

—

” “Thu, 24 Oct 2024

pfSense 2.5.2 Cross Site Scripting

A cross site scripting vulnerability in pfsense version 2.5.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the $pconfig variable at interfaces_groups_edit.php.

- Link

—

” “Wed, 23 Oct 2024

ABB Cylon Aspect 3.08.01 logCriticalLookup.php Unauthenticated Log Disclosure

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated log information disclosure vulnerability. An unauthorized attacker can reference the affected page and disclose the webserver’s log file containing system information running on the device.

- Link

—

” “Wed, 23 Oct 2024

ABB Cylon Aspect 3.08.01 throttledLog.php Unauthenticated Log Disclosure

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated log information disclosure vulnerability. An unauthorized attacker can reference the affected page and disclose the webserver’s log file containing system information running on the device.

- Link

—

” “Tue, 22 Oct 2024

ABB Cylon Aspect 3.08.01 persistenceManagerAjax.php Command Injection

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the directory HTTP POST parameter called by the persistenceManagerAjax.php script.

- Link

—

” “Tue, 22 Oct 2024

Linux Dangling PFN Mapping / Use-After-Free

An error path in usbdev_mmap() (where remap_pfn_range() fails midway through) frees pages before the PFN mapping pointing to those pages is cleaned up, making physical page use-after-free possible. Some other drivers look like they might have similar issues.

- Link

—

” “Mon, 21 Oct 2024

Rittal IoT Interface / CMC III Processing Unit Signature Verification / Session ID

Rittal IoT Interface and CMC III Processing Unit versions prior to 6.21.00.2 suffer from improper signature verification and predictable session identifier vulnerabilities.

- Link

—

” “Fri, 18 Oct 2024

Magento / Adobe Commerce Remote Code Execution

This Metasploit module uses a combination of an arbitrary file read (CVE-2024-34102) and a buffer overflow in glibc (CVE-2024-2961). It allows for unauthenticated remote code execution on various versions of Magento and Adobe Commerce (and earlier versions if the PHP and glibc versions are also vulnerable). Versions affected include 2.4.7 and earlier, 2.4.6-p5 and earlier, 2.4.5-p7 and earlier, and 2.4.4-p8 and earlier.

- Link

—

” “Fri, 18 Oct 2024

ABB Cylon Aspect 3.08.01 databaseFileDelete.php Command Injection

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the file HTTP POST parameter called by the databaseFileDelete.php script.

- Link

—

” “Fri, 18 Oct 2024

IBM Security Verify Access 10.0.8 Open Redirection

IBM Security Verify Access versions 10.0.0 through 10.0.8 suffer from an OAUTH related open redirection vulnerability.

- Link

—

” “Thu, 17 Oct 2024

ABB Cylon Aspect 3.08.01 networkDiagAjax.php Remote Network Utility Execution

ABB Cylon Aspect version 3.08.01 allows an unauthenticated attacker to perform network operations such as ping, traceroute, or nslookup on arbitrary hosts or IPs by sending a crafted GET request to networkDiagAjax.php. This could be exploited to interact with or probe internal or external systems, leading to internal information disclosure and misuse of network resources.

- Link

—

” “Thu, 17 Oct 2024

SofaWiki 3.9.2 Cross Site Scripting

SofaWiki version 3.9.2 suffers from a reflective cross site scripting vulnerability.

- Link

—

” “Thu, 17 Oct 2024

SofaWiki 3.9.2 Cross Site Scripting

SofaWiki version 3.9.2 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Thu, 17 Oct 2024

SofaWiki 3.9.2 Shell Upload

SofaWiki version 3.9.2 suffers from a remote shell upload vulnerability.

- Link

—

” “Wed, 16 Oct 2024

BYOB Unauthenticated Remote Code Execution

This Metasploit module exploits two vulnerabilities in the BYOB (Build Your Own Botnet) web GUI. It leverages an unauthenticated arbitrary file write that allows modification of the SQLite database, adding a new admin user. It also uses an authenticated command injection in the payload generation page. These vulnerabilities remain unpatched.

- Link

—

” “Wed, 16 Oct 2024

ABB Cylon Aspect 3.08.01 mapConfigurationDownload.php Configuration Download

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated configuration download vulnerability. This can be exploited to download the SQLite DB that contains the configuration mappings information via the FTControlServlet by directly calling the mapConfigurationDownload.php script.

- Link

—

” “Tue, 15 Oct 2024

ABB Cylon Aspect 3.08.00 sslCertAjax.php Remote Command Execution

ABB Cylon Aspect version 3.08.00 suffers from an authenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the country, state, locality, organization, and hostname HTTP POST parameters called by the sslCertAjax.php script.

- Link

—

” “Tue, 15 Oct 2024

Dolibarr 20.0.1 SQL Injection

Dolibarr version 20.0.1 suffers from a remote SQL injection vulnerability.

- Link

—

” “Tue, 15 Oct 2024

WatchGuard XTM Firebox 12.5.x Buffer Overflow

WatchGuard XTM Firebox version 12.5.x suffers from a buffer overflow vulnerability.

- Link

—

” “Tue, 15 Oct 2024

msm 5.15 Arbitrary Kernel Address Access

This bug was found in msm-5.15 using tag KERNEL.PLATFORM.2.1.r1-05400-kernel.0. The fastrpc_file struct contains a flag, is_compat, that is set if the 32-bit compat_ioctl vfs handler is ever called on a fastrpc file (e.g. by opening and ioctling on /dev/adsprpc-smd). This flag is later used inside of e.g. fastrpc_internal_invoke2's macro invocations of K_COPY_FROM_USER to make decisions about whether the provided pointer is a userland pointer or a kernel-land pointer. However, because the state for making this K_COPY_FROM_USER decision is stored within the broadly accessible fastrpc_file struct instead of stored per ioctl invocation, this means that 64-bit ioctl invocations of fastrpc_internal_invoke2 will use userland provided addresses as kernel pointers if the 32-bit ioctl interface of the same fastrpc_file was ever previously invoked. This leads directly to attacker-controlled reads of arbitrary kernel addresses.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Thu, 24 Oct 2024

ZDI-24-1422: Nikon NEF Codec Thumbnail Provider NRW File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Wed, 23 Oct 2024

ZDI-24-1421: VMware HCX listExtensions SQL Injection Remote Code Execution Vulnerability

- Link

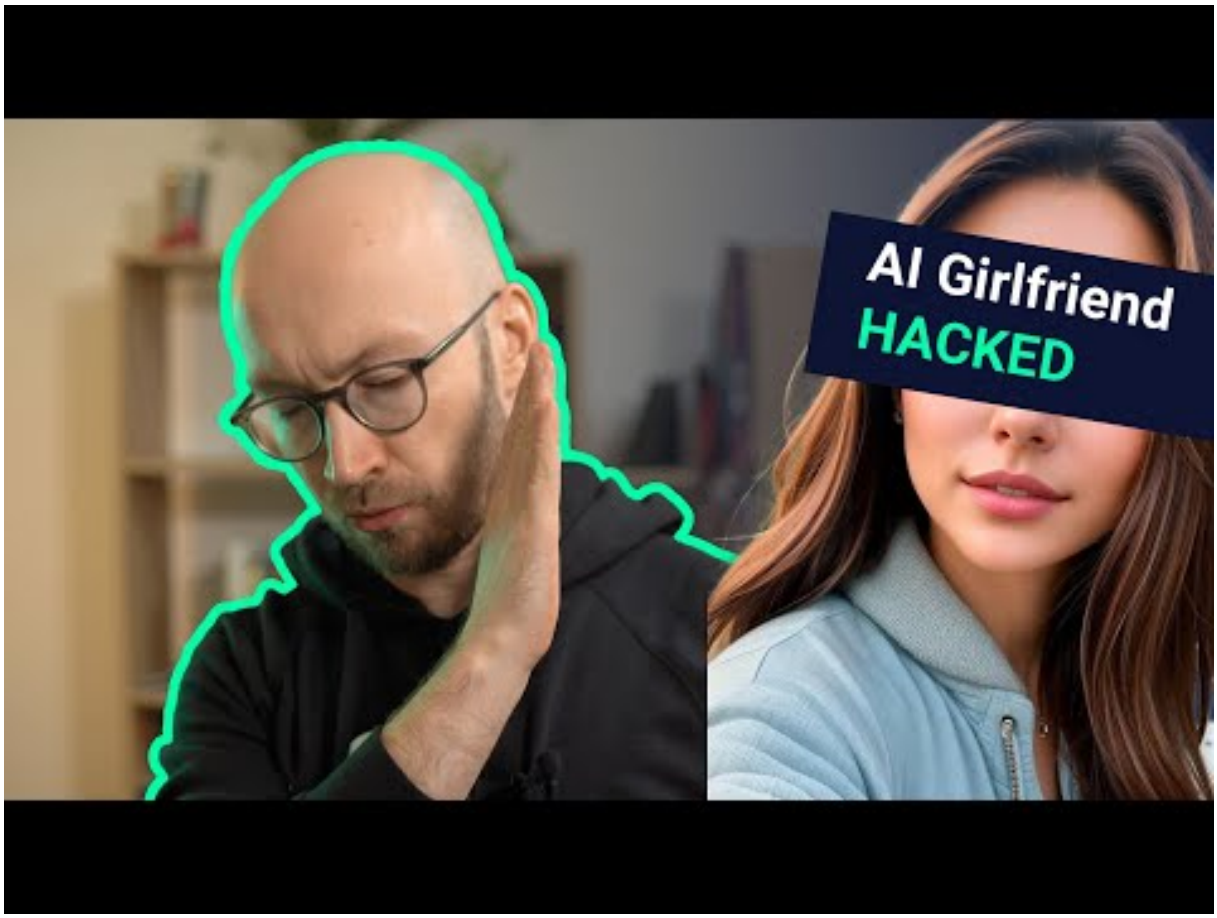
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 AI Girlfriends HACKED (Da steht uns noch was bevor)



Zum Youtube Video

6 Cyberangriffe: (Okt)

Datum	Opfer	Land	Information
2024-10-24	Libération	[FRA]	Link
2024-10-24	OneLog	[CHE]	Link
2024-10-24	Idea	[DEU]	Link
2024-10-23	Landkreis Kitzingen	[DEU]	Link
2024-10-22	Sabesp (Companhia de Saneamento Básico do Estado de São Paulo)	[BRA]	Link
2024-10-22	Isa SpA	[ITA]	Link
2024-10-20	District scolaire public de Winnebago	[USA]	Link
2024-10-19	La Coopérative d'Exploitation et de Répartition Pharmaceutique (CERP) Bretagne-Atlantique	[FRA]	Link
2024-10-18	Grupo Aeroportuario del Centro Norte (OMA)	[MEX]	Link
2024-10-18	Air-e	[COL]	Link
2024-10-18	Karat Packaging Inc.	[USA]	Link
2024-10-17	Formpipe	[DNK]	Link
2024-10-17	Conseil scolaire Viamonde	[CAN]	Link
2024-10-15	aap Implantate AG	[DEU]	Link
2024-10-15	Comune di Aversa	[ITA]	Link
2024-10-15	Fédération suisse de gymnastique	[CHE]	Link
2024-10-14	La mairie de Clairefontaine-en-Yvelines	[FRA]	Link
2024-10-14	Well Chip Group Berhad	[MYS]	Link
2024-10-14	Sorso	[ITA]	Link
2024-10-14	Université de Moncton	[CAN]	Link
2024-10-13	Johannesstift-Diakonie Berlin	[DEU]	Link
2024-10-13	Mutuelle d'Ivry (Mif)	[FRA]	Link
2024-10-11	Calgary Public Library (CPL)	[CAN]	Link

Datum	Opfer	Land	Information
2024-10-11	Polar	[FIN]	Link
2024-10-10	Guajará-Mirim	[BRA]	Link
2024-10-10	Agence pour la Modernisation Administrative (AMA) du Portugal	[PRT]	Link
2024-10-09	Healthcare Services Group (HSG)	[USA]	Link
2024-10-08	Elbe-Heide	[DEU]	Link
2024-10-08	Nevada Joint Union High School District (NJUHSD)	[USA]	Link
2024-10-08	Les Chambres d'agriculture de Normandie	[FRA]	Link
2024-10-07	Vermilion Parish School System	[USA]	Link
2024-10-07	Axis Health System	[USA]	Link
2024-10-07	Teddy	[ITA]	Link
2024-10-05	Casio Computer Co.	[JPN]	Link
2024-10-04	Groupe Hospi Grand Ouest	[FRA]	Link
2024-10-04	Cabot Financial	[IRL]	Link
2024-10-03	Uttarakhand	[IND]	Link
2024-10-03	American Water Works	[USA]	Link
2024-10-02	Thoraxzentrum Bezirk Unterfranken	[DEU]	Link
2024-10-02	Wayne County	[USA]	Link
2024-10-02	Traffics GmbH	[DEU]	Link
2024-10-02	Berufsschule de Schaffhausen	[CHE]	Link
2024-10-01	Oyonnax	[FRA]	Link
2024-10-01	C.R. Laurence (CRL)	[USA]	Link

7 Ransomware-Erpressungen: (Okt)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-27	[Edmov]	killsec	Link
2024-10-26	[TV Guide Magazine]	play	Link
2024-10-26	[Positive Business Solutions]	play	Link
2024-10-26	[C & C Industries]	play	Link
2024-10-26	[wescan-services.com 760 GB]	blacksuit	Link
2024-10-26	[Westwood Country Club]	meow	Link
2024-10-26	[PT Transportasi Gas Indonesia]	meow	Link
2024-10-26	[The Eye Clinic Surgicenter]	meow	Link
2024-10-26	[Bliss Worldwide]	killsec	Link
2024-10-26	[wescan-services.com]	blacksuit	Link
2024-10-26	[Legacy Treatment Services]	interlock	Link
2024-10-26	[Premier Work Support]	bianlian	Link
2024-10-25	[www.olanocorp.com]	ransomhub	Link
2024-10-25	[Doctor24x7]	killsec	Link
2024-10-25	[Delcaper]	killsec	Link
2024-10-25	[Government of Brazil]	killsec	Link
2024-10-25	[NoBroker]	killsec	Link
2024-10-25	[SW Reclaim]	killsec	Link
2024-10-25	[Wilson Tarquin]	killsec	Link
2024-10-25	[Ottawa Valley Handrailing Company Ltd]	nitrogen	Link
2024-10-25	[Evergreen Public Schools (evergreenps.org)]	fog	Link
2024-10-25	[hcsgcorp.com]	underground	Link
2024-10-25	[SRS-Stahl GmbH]	sarcoma	Link
2024-10-25	[MESHWORKS]	sarcoma	Link
2024-10-25	[De Rose Lawyers]	rhysida	Link
2024-10-25	[Matouk Bassiouny]	raworld	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-25	[Cucamonga Valley Water District (cvwdwater.com)]	fog	Link
2024-10-25	[Evergreen Local School District (evgvikings.org)]	fog	Link
2024-10-25	[lolaliza.com]	blacksuit	Link
2024-10-25	[Ambica Steels]	hunters	Link
2024-10-25	[Niko Resources Ltd.]	hunters	Link
2024-10-16	[ValueMax Group]	lynx	Link
2024-10-16	[Precision Electrical Systems]	lynx	Link
2024-10-16	[Denkali]	lynx	Link
2024-10-25	[The Knesset - Israel]	hellcat	Link
2024-10-25	[HUBBARDHALL.COM]	clop	Link
2024-10-25	[deschampsimp.com]	blacksuit	Link
2024-10-25	[omara-ag.com]	blacksuit	Link
2024-10-25	[nrcs.net]	blacksuit	Link
2024-10-25	[Ferrer & Ojeda]	sarcoma	Link
2024-10-25	[Groupseco.com]	ransomhub	Link
2024-10-25	[zyloware.com]	blacksuit	Link
2024-10-25	[unitedsprinkler.com]	blacksuit	Link
2024-10-24	[Centrillion Technologies]	cicada3301	Link
2024-10-25	[Spine by Villamil MD]	everest	Link
2024-10-25	[Aspen Healthcare]	everest	Link
2024-10-25	[Pacific Pulmonary Medical Group]	everest	Link
2024-10-24	[Digital Engineering]	raworld	Link
2024-10-24	[www.resourceinternational.com]	ransomhub	Link
2024-10-23	[bulloch.solutions]	ransomhub	Link
2024-10-24	[www.kciconst.com]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-24	[McElroy, Quirk & Burch, APC]	bianlian	Link
2024-10-18	[www.oma.aero]	ransomhub	Link
2024-10-24	[Drug and Alcohol Treatment Service]	interlock	Link
2024-10-24	[tuggleduggins.com]	blackbasta	Link
2024-10-24	[Value City NJ (valuecitynj.com)]	fog	Link
2024-10-24	[The Getz Group (getz.com.hk)]	fog	Link
2024-10-24	[pkaufmann.com]	apt73	Link
2024-10-24	[modplan.co.uk]	apt73	Link
2024-10-24	[hpecds.com]	apt73	Link
2024-10-24	[carolinaarthritis.com]	threeam	Link
2024-10-24	[Smeg]	interlock	Link
2024-10-24	[Apache Mills, Inc. (apachemills.com)]	fog	Link
2024-10-23	[thompsoncreek.com]	apt73	Link
2024-10-23	[www.northernsafety.com]	apt73	Link
2024-10-23	[mgfsourcing.com]	apt73	Link
2024-10-17	[appen.com]	apt73	Link
2024-10-17	[filmai.in]	apt73	Link
2024-10-17	[drizly.com]	apt73	Link
2024-10-17	[robinhood.com]	apt73	Link
2024-10-21	[thebeautyclick.co.uk]	apt73	Link
2024-10-21	[trans-logik.com]	apt73	Link
2024-10-21	[www.talonsolutions.co.uk]	apt73	Link
2024-10-21	[Sandro Forte Financial Support]	apt73	Link
2024-10-21	[Susan Fischgrund]	apt73	Link
2024-10-21	[nanolive.ch]	apt73	Link
2024-10-24	[picsolve.com]	cactus	Link
2024-10-24	[bcllegal.com]	cactus	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-24	[lifeminetx.com]	lynx	Link
2024-10-24	[LifeMine]	lynx	Link
2024-10-24	[Iron World Manufacturing]	play	Link
2024-10-24	[Eagle Industries]	play	Link
2024-10-24	[Action Heating & Cooling]	play	Link
2024-10-24	[Mainelli Mechanical Contractors]	play	Link
2024-10-24	[TU Parks]	play	Link
2024-10-24	[Ivanhoe Club]	play	Link
2024-10-23	[Prince Pipes]	raworld	Link
2024-10-23	[P+B Team Aircargo]	raworld	Link
2024-10-23	[Gluckstein Personal Injury Lawyers]	bianlian	Link
2024-10-23	[The Povman Law Firm]	bianlian	Link
2024-10-14	[passivecomponent.com]	ransomhub	Link
2024-10-23	[By Design LLC]	meow	Link
2024-10-23	[Wayne County]	interlock	Link
2024-10-23	[Youngs Timber Builders Merchants]	meow	Link
2024-10-23	[Goshen Central School District (gcsny.org)]	fog	Link
2024-10-23	[Mar-Bal (mar-bal.com)]	fog	Link
2024-10-23	[KEE Process]	meow	Link
2024-10-23	[Easterseals]	rhysida	Link
2024-10-18	[elnamagnetics.com]	ransomhub	Link
2024-10-23	[Tricon Energy]	lynx	Link
2024-10-23	[shipkar.co.in]	killsec	Link
2024-10-22	[IdeaLab]	hunters	Link
2024-10-22	[Lincoln University (lincolnu.edu)]	fog	Link
2024-10-22	[Clear Connection (clearconnection.com)]	fog	Link
2024-10-22	[Aerotecnic]	blacksuit	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-21	[Precision Steel Services]	spacebears	Link
2024-10-22	[tkg.com]	ransomhub	Link
2024-10-22	[lpahorticole.faylbillot.educagri.fr]	ransomhub	Link
2024-10-22	[bwdtechnology.com]	ransomhub	Link
2024-10-16	[davisbrothersinc.com]	ransomhub	Link
2024-10-22	[polypane.be]	ransomhub	Link
2024-10-22	[dennissupply.com]	ransomhub	Link
2024-10-22	[specpro-inc.com]	ransomhub	Link
2024-10-22	[semna.fr]	ransomhub	Link
2024-10-22	[1doc.sg]	ransomhub	Link
2024-10-22	[Automha]	medusa	Link
2024-10-22	[American Mechanical, inc]	medusa	Link
2024-10-22	[American Medical Billing]	medusa	Link
2024-10-17	[mauguio-carnon.com]	ransomhub	Link
2024-10-09	[donbosco-landser.net]	ransomhub	Link
2024-10-22	[boloforms.com]	killsec	Link
2024-10-22	[onedayevent.com]	killsec	Link
2024-10-22	[autodukan.com]	killsec	Link
2024-10-21	[fordcountrymotors.mx]	lockbit3	Link
2024-10-21	[temple-inc.com]	blackbasta	Link
2024-10-21	[milleredge.com]	blackbasta	Link
2024-10-21	[gkcorp.com]	blackbasta	Link
2024-10-21	[ssbwc.com]	blackbasta	Link
2024-10-21	[lewa.com]	blackbasta	Link
2024-10-04	[City Of Forest Park]	monti	Link
2024-10-21	[Burgess Kilpatrick]	monti	Link
2024-10-21	[Welding and Fabrication (Humble Mfg)]	monti	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-21	[Raeyco Lab Equipment]	monti	Link
2024-10-21	[La Tazza D'oro]	monti	Link
2024-10-21	[Teddy SpA]	blacksuit	Link
2024-10-21	[www.stivo.com]	ransomhub	Link
2024-10-21	[Schweiger Transport (schweiger-gmbh.de)]	fog	Link
2024-10-21	[Philadelphia Macaroni (philamacaroni.com)]	fog	Link
2024-10-21	[yorozu-corp.co.jp]	ransomhub	Link
2024-10-21	[Mercury Theatre]	hunters	Link
2024-10-21	[Trimarc Financial (trimarc.com)]	fog	Link
2024-10-21	[Arango Billboard]	meow	Link
2024-10-21	[Sanglier Limited]	meow	Link
2024-10-20	[qs-group.com]	ransomhub	Link
2024-10-20	[Interbel]	arcusmedia	Link
2024-10-20	[Petropolis Pet Resort]	arcusmedia	Link
2024-10-20	[Superior Quality Insurance Agency]	arcusmedia	Link
2024-10-20	[Vasesa]	arcusmedia	Link
2024-10-20	[Country Club El Bosque]	arcusmedia	Link
2024-10-20	[Atende Software's]	hunters	Link
2024-10-20	[apollohospitals.com]	killsec	Link
2024-10-14	[mh-mech.com]	ransomhub	Link
2024-10-19	[sizeloveconstruction.com]	ransomhub	Link
2024-10-19	[rcschools.net]	blacksuit	Link
2024-10-19	[mopsohio.com]	blacksuit	Link
2024-10-19	[Kansas City Hospice]	blacksuit	Link
2024-10-19	[KMC Controls]	hunters	Link
2024-10-19	[Michael J Gurfinkel]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-19	[SPECTRUMCHEMICAL.COM]	clop	Link
2024-10-19	[clinicia.com]	ransomhub	Link
2024-10-19	[paciente.sempremedico.com.br]	ransomhub	Link
2024-10-19	[starhealth.in]	ransomhub	Link
2024-10-19	[T-Space]	cicada3301	Link
2024-10-19	[Pheim Unit Trusts Berhad]	sarcoma	Link
2024-10-19	[Zierick Manufacturing Corporation]	sarcoma	Link
2024-10-19	[Open Range Field Services]	sarcoma	Link
2024-10-19	[ask.vet]	killsec	Link
2024-10-19	[Country Inn & Suites by Radisson]	everest	Link
2024-10-17	[Wilkinson]	play	Link
2024-10-18	[Mid State Electric]	play	Link
2024-10-18	[Absolute Machine Tools]	play	Link
2024-10-18	[McCody]	play	Link
2024-10-18	[The Strainrite Companies]	play	Link
2024-10-05	[INDIBA Group]	cicada3301	Link
2024-10-16	[Astolabs.com]	ransomhub	Link
2024-10-18	[Fromm (FrommBeauty.com)]	fog	Link
2024-10-18	[Ultra Tune (ultratune.com.au)]	fog	Link
2024-10-18	[Alqaryahauction.com]	ransomhub	Link
2024-10-18	[www.qal.com]	ransomhub	Link
2024-10-18	[CreaGen Inc]	everest	Link
2024-10-17	[Dubin Group]	cicada3301	Link
2024-10-17	[RDC Control Ltd]	cicada3301	Link
2024-10-17	[Racing Forensics Inc]	cicada3301	Link
2024-10-17	[Luxwood Software Tools]	cicada3301	Link
2024-10-18	[tripxoxo.com]	killsec	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-17	[www.proflex.ro]	ransomhub	Link
2024-10-17	[www.chiltonisd.org]	ransomhub	Link
2024-10-03	[www.kersey.net]	ransomhub	Link
2024-10-02	[www.aristoiclassical.org]	ransomhub	Link
2024-10-03	[www.camelotservices.com]	ransomhub	Link
2024-10-17	[HiCare.net]	ransomhub	Link
2024-10-17	[Bigpharmacy.com.my]	ransomhub	Link
2024-10-17	[Auxit S.r.l]	sarcoma	Link
2024-10-17	[volohealth.in]	killsec	Link
2024-10-17	[W?l?????n]	play	Link
2024-10-16	[Fractal ID]	stormous	Link
2024-10-02	[Funlab]	lynx	Link
2024-10-09	[Tankstar]	lynx	Link
2024-10-16	[Welker (welker.com)]	fog	Link
2024-10-16	[Cordogan Clark and Associates (cordoganclark.com)]	fog	[Link]((cordoganclark.co
2024-10-15	[powiatjedrzejow.pl]	ransomhub	Link
2024-10-16	[Astolabs.com ASTO LABS]	ransomhub	Link
2024-10-16	[transport-system.com]	ransomhub	Link
2024-10-16	[DoctorsToYou.com]	ransomhub	Link
2024-10-16	[Horsesportireland.ie]	ransomhub	Link
2024-10-16	[Food Sciences Corporation (foodsciences.com)]	fog	Link
2024-10-16	[synertrade.com]	cactus	Link
2024-10-16	[G-plans.com]	ransomhub	Link
2024-10-16	[Fpapak.org]	ransomhub	Link
2024-10-16	[CETRULO]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-16	[Nor-Well]	play	Link
2024-10-16	[Kuhn and Associates]	play	Link
2024-10-16	[moi.gov.ly]	killsec	Link
2024-10-16	[Corporate Job Bank]	bianlian	Link
2024-10-16	[Lein Law Offices]	bianlian	Link
2024-10-15	[Boston Children’s Health Physicians]	bianlian	Link
2024-10-15	[Henry County Schools]	rhysida	Link
2024-10-15	[Central Pennsylvania Food Bank]	fog	Link
2024-10-15	[In the depths of software development.]	abyss	Link
2024-10-15	[Promise Technology, Inc.]	abyss	Link
2024-10-15	[basarsoft.com.tr]	ransomhub	Link
2024-10-15	[Ideker]	medusa	Link
2024-10-15	[Ultimate Removal]	medusa	Link
2024-10-15	[Inner City Education Foundation]	medusa	Link
2024-10-15	[SystemPavers]	medusa	Link
2024-10-15	[McMunn & Yates Building Suppliesorp]	sarcoma	Link
2024-10-15	[Microworks]	rhysida	Link
2024-10-15	[Parnell Defense]	hunters	Link
2024-10-15	[Aaren Scientific]	hunters	Link
2024-10-15	[Nora Biscuits]	play	Link
2024-10-15	[Rescar Companies]	play	Link
2024-10-15	[Concord]	play	Link
2024-10-15	[OzarksGo]	play	Link
2024-10-14	[Byerly Aviation]	play	Link
2024-10-14	[Courtney Construction]	play	Link
2024-10-14	[rudrakshahospitals.com]	killsec	Link
2024-10-14	[AOSense]	stormous	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-14	[Henneman Engineering]	play	Link
2024-10-14	[Misionero Vegetables]	play	Link
2024-10-14	[Steel Art Signs]	play	Link
2024-10-14	[Ascires]	stormous	Link
2024-10-14	[Astero]	meow	Link
2024-10-14	[gfm-uk.com]	blackbasta	Link
2024-10-14	[caseparts.com]	blackbasta	Link
2024-10-14	[compra-aruba.com]	ElDorado	Link
2024-10-14	[Durham Region]	dragonforce	Link
2024-10-13	[medicato.com]	ransomhub	Link
2024-10-02	[FUN-LAB]	lynx	Link
2024-10-13	[Cathexis Holdings LP]	interlock	Link
2024-10-11	[Ascires Biomedical Group]	stormous	Link
2024-10-13	[Rocky Mountain Gastroenterology]	meow	Link
2024-10-11	[World Vision Perú]	medusa	Link
2024-10-11	[Construction Systems inc]	medusa	Link
2024-10-13	[Timber]	sarcoma	Link
2024-10-12	[saizeriya.co.jp]	ransomhub	Link
2024-10-12	[Modiin Ezrachi]	meow	Link
2024-10-12	[OSG Tool]	meow	Link
2024-10-11	[NextStage.AI]	ransomhub	Link
2024-10-11	[Protective Industrial Products]	hunters	Link
2024-10-11	[Therabel Lucien Pharma SAS]	hunters	Link
2024-10-11	[Rumpke Consolidated Companies]	hunters	Link
2024-10-11	[Østerås Bygg]	medusa	Link
2024-10-11	[Unita Turism]	meow	Link
2024-10-11	[Elmore Goldsmith]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-11	[promise.com]	abyss	Link
2024-10-11	[peorialawyers.com]	ransomhub	Link
2024-10-10	[extramarks.com]	killsec	Link
2024-10-10	[Doctors Regional Cancer Center]	incransom	Link
2024-10-10	[oklahomasleepinstitute.co]	threeam	Link
2024-10-10	[Axis Health System]	rhysida	Link
2024-10-10	[The Law Office of Omar O Vargas]	meow	Link
2024-10-10	[Structural and Steel Products]	hunters	Link
2024-10-10	[medexhco.com]	ransomhub	Link
2024-10-10	[La Futura]	meow	Link
2024-10-10	[Barnes Cohen and Sullivan]	meow	Link
2024-10-10	[Atlantic Coast Consulting Inc]	meow	Link
2024-10-10	[Glacier]	hunters	Link
2024-10-09	[Casio Computer Co., Ltd]	underground	Link
2024-10-10	[Doscast]	handala	Link
2024-10-09	[FortyEighty Architecture]	play	Link
2024-10-09	[RobbJack & Crystallume]	play	Link
2024-10-09	[Universal Companies]	play	Link
2024-10-09	[argofinance.org]	killsec	Link
2024-10-09	[transfoodbeverage.com]	killsec	Link
2024-10-09	[InCare Technologies]	sarcoma	Link
2024-10-09	[Antenne Reunion Radio]	sarcoma	Link
2024-10-09	[Smart Media Group Bulgaria]	sarcoma	Link
2024-10-09	[The Roberts Family Law Firm]	sarcoma	Link
2024-10-09	[Gedco]	sarcoma	Link
2024-10-09	[EARTHWORKS Group]	sarcoma	Link
2024-10-09	[Perfection Fresh]	sarcoma	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-09	[Advanced Accounting & Business Advisory]	sarcoma	Link
2024-10-09	[Road Distribution Services]	sarcoma	Link
2024-10-09	[Lácteos Lorán]	sarcoma	Link
2024-10-09	[Curtidos Barbero]	sarcoma	Link
2024-10-09	[EasyPay]	sarcoma	Link
2024-10-09	[Jumbo Electronics Qatar]	sarcoma	Link
2024-10-09	[Navarra & Marzano]	sarcoma	Link
2024-10-09	[Costa Del Sol Hotels]	sarcoma	Link
2024-10-09	[The Plastic Bag]	sarcoma	Link
2024-10-09	[Elevator One]	sarcoma	Link
2024-10-09	[March Elevator]	sarcoma	Link
2024-10-09	[Suntrust Properties]	sarcoma	Link
2024-10-09	[tankstar.com]	lynx	Link
2024-10-09	[victrongroup.com]	abyss	Link
2024-10-09	[FULTON.COM]	clop	Link
2024-10-08	[Orbit Software, Inc.]	dragonforce	Link
2024-10-09	[avans.com]	killsec	Link
2024-10-08	[Eagle Recovery Associates]	play	Link
2024-10-08	[AnVa Industries]	play	Link
2024-10-08	[Smoker’s Choice]	play	Link
2024-10-08	[Saratoga Liquor]	play	Link
2024-10-08	[Accounting Resource Group]	play	Link
2024-10-08	[pingan.com]	killsec	Link
2024-10-08	[Ambassador of Israel in Germany Emails]	handala	Link
2024-10-08	[Aaren Scientific]	play	Link
2024-10-04	[blalockcompanies.com]	ransomhub	Link
2024-10-08	[Advantage CDC]	meow	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-08	[Trinity Wholesale Distributors Inc]	meow	Link
2024-10-08	[okcabstract.com]	ransomhub	Link
2024-10-08	[Blain Supply]	lynx	Link
2024-10-07	[Sit & Sleep]	lynx	Link
2024-10-08	[AIUT]	hunters	Link
2024-10-08	[Maxdream]	meow	Link
2024-10-08	[matki.co.uk]	cactus	Link
2024-10-08	[corporatejobbank.com]	cactus	Link
2024-10-08	[Davis Pickren Seydel and Sneed LLP]	meow	Link
2024-10-08	[Accurate Railroad Construction Ltd]	meow	Link
2024-10-08	[Max Shop]	handala	Link
2024-10-07	[autodoc.pro]	ransomhub	Link
2024-10-06	[trulysmall.com]	ransomhub	Link
2024-10-07	[nspproteins.com]	ransomhub	Link
2024-10-08	[The Superior Court of California]	meow	Link
2024-10-08	[healthyuturn.in]	killsec	Link
2024-10-08	[uccretrievals.com]	ElDorado	Link
2024-10-08	[premierpackaging.com]	ElDorado	Link
2024-10-08	[htetech.com]	ElDorado	Link
2024-10-08	[goughconstruction.com]	ElDorado	Link
2024-10-08	[fleetequipment.com]	ElDorado	Link
2024-10-08	[auto-recyclers.com]	ElDorado	Link
2024-10-08	[atd-american.com]	ElDorado	Link
2024-10-08	[allianceind.com]	ElDorado	Link
2024-10-08	[avioesforza.it]	ElDorado	Link
2024-10-08	[tankerska.hr]	ElDorado	Link
2024-10-08	[totalelectronics.com]	ElDorado	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-07	[Istrail]	medusa	Link
2024-10-07	[Albany College of Pharmacy]	medusa	Link
2024-10-07	[Arelance Group]	medusa	Link
2024-10-08	[Pearl Cohen]	bianlian	Link
2024-10-07	[Broward Realty Corp]	everest	Link
2024-10-07	[yassir.com]	killsec	Link
2024-10-03	[tpgagedcare.com.au]	lockbit3	Link
2024-10-06	[IIB (Israeli Industrial Batteries) Leaked]	handala	Link
2024-10-03	[lyra.officegroup]	stormous	Link
2024-10-05	[AOSense/NASA]	stormous	Link
2024-10-05	[NASA/AOSense]	stormous	Link
2024-10-05	[Creative Consumer Concepts]	play	Link
2024-10-05	[Power Torque Services]	play	Link
2024-10-05	[seoulpi.io]	killsec	Link
2024-10-05	[canstarrestorations.com]	ransomhub	Link
2024-10-05	[www.ravencm.com]	ransomhub	Link
2024-10-05	[Ibermutuamur]	hunters	Link
2024-10-05	[betterhalf.ai]	killsec	Link
2024-10-05	[HARTSON-KENNEDY.COM]	clop	Link
2024-10-04	[omniboxx.nl]	ransomhub	Link
2024-10-05	[BNBuilders]	hunters	Link
2024-10-03	[winwinza.com]	ransomhub	Link
2024-10-04	[Storck-Baugesellschaft mbH]	incransom	Link
2024-10-04	[C&L Ward]	play	Link
2024-10-04	[Wilmington Convention Center]	play	Link
2024-10-04	[Guerriere & Halnon]	play	Link
2024-10-04	[Markdom Plastic Products]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-04	[Pete’s Road Service]	play	Link
2024-10-03	[releese.io]	ransomhub	Link
2024-10-04	[kleberandassociates.com]	ransomhub	Link
2024-10-04	[City Of Forest Park - Full Leak]	monti	Link
2024-10-04	[Riley Gear Corporation]	akira	Link
2024-10-04	[TANYA Creations]	akira	Link
2024-10-04	[mullenwylie.com]	ElDorado	Link
2024-10-04	[CopySmart LLC]	ciphbit	Link
2024-10-04	[North American Breaker]	akira	Link
2024-10-04	[Amplitude Laser]	hunters	Link
2024-10-04	[GW Mechanical]	hunters	Link
2024-10-04	[Dreyfuss + Blackford Architecture]	hunters	Link
2024-10-04	[Transtec SAS]	orca	Link
2024-10-02	[enterpriseoutsourcing.com]	ransomhub	Link
2024-10-04	[DPC DATA]	qilin	Link
2024-10-03	[Lyomark Pharma]	dragonforce	Link
2024-10-03	[Conductive Containers, Inc]	cicada3301	Link
2024-10-04	[bbgc.gov.bd]	killsec	Link
2024-10-03	[CobelPlast]	hunters	Link
2024-10-03	[Shin Bet]	handala	Link
2024-10-03	[Barnes & Cohen]	trinity	Link
2024-10-03	[TRC Worldwide Engineering (Trcww)]	akira	Link
2024-10-03	[Rob Levine & Associates (roblevine.com)]	akira	Link
2024-10-03	[Red Barrels]	nitrogen	Link
2024-10-03	[CaleyWray]	hunters	Link
2024-10-03	[LIFTING.COM]	clop	Link
2024-10-01	[Emerson]	medusa	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-02	[ETC Companies]	akira	Link
2024-10-02	[Holmes & Brakel]	akira	Link
2024-10-02	[Forshey Prostok LLP]	qilin	Link
2024-10-02	[Israel Prime Minister Emails]	handala	Link
2024-10-02	[FoccoERP]	trinity	Link
2024-10-01	[Quantum Healthcare]	incransom	Link
2024-10-01	[United Animal Health]	qilin	Link
2024-10-01	[Akromold]	nitrogen	Link
2024-10-01	[Labib Funk Associates]	nitrogen	Link
2024-10-01	[Research Electronics International]	nitrogen	Link
2024-10-01	[Cascade Columbia Distribution]	akira	Link
2024-10-01	[ShoreMaster]	akira	Link
2024-10-01	[marthamedeiros.com.br]	madliberator	Link
2024-10-01	[CSG Consultants]	akira	Link
2024-10-01	[aberdeenwa.gov]	ElDorado	Link
2024-10-01	[Corantioquia]	meow	Link
2024-10-01	[performance-therapies]	qilin	Link
2024-10-01	[www.galab.com]	cactus	Link
2024-10-01	[telehealthcenter.in]	killsec	Link
2024-10-01	[howardcpas.com]	ElDorado	Link
2024-10-01	[bshsoft.com]	ElDorado	Link
2024-10-01	[credihealth.com]	killsec	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.