
Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241031



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)	21
8 Quellen	39
8.1 Quellenverzeichnis	39
9 Impressum	40

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

Jetzt patchen! Ransomware-Attacken auf Server mit CyberPanel beobachtet

Angreifer nutzen kritische Schwachstellen in Servern aus, auf denen CyberPanel installiert ist. Eine abgesicherte Version ist verfügbar.

- [Link](#)

—

Qnap schließt NAS-Sicherheitslücke aus Hackerwettbewerb

NAS-Modelle von Qnap mit der Backupsoftware HBS 3 Hybrid Backup Sync sind angreifbar. Eine neue Version schließt eine kritische Schwachstelle.

- [Link](#)

—

Google Chrome: Kritische Sicherheitslücke gestopft

Das wöchentliche Update für Googles Chrome-Webbrowser schließt dieses Mal eine als kritisches Risiko eingestufte Sicherheitslücke.

- [Link](#)

—

Sicherheitsupdates: Firefox und Thunderbird gegen Schadcode-Attacken gerüstet

Angreifer können die Browser Firefox und Firefox ESR und den Mailclient Thunderbird unter anderem abstürzen lassen.

- [Link](#)

—

IBM App Connect Enterprise: Angreifer können Anmeldung umgehen

Die Entwickler von IBM haben zwei Sicherheitslücken in App Connect Enterprise Certified Container geschlossen. Attacken sind aber nicht ohne Weiteres möglich.

- [Link](#)

—

VMware Tanzu Spring Security: Umgehung von Autorisierungsregeln möglich

In VMware Tanzu Spring Security klafft eine kritische Sicherheitslücke, die Angreifern die Umgehung von Autorisierungsregeln ermöglicht.

- [Link](#)

—

Nvidia: Rechteausweitung durch Sicherheitslücken in Grafiktreiber möglich

Nvidia warnt vor mehreren Sicherheitslücken in den Grafiktreibern, die etwa das Ausweiten der Rechte ermöglichen. Updates stehen bereit.

- [Link](#)

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](#)

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	0.994970000	Link
CVE-2023-6895	0.925010000	0.990810000	Link
CVE-2023-6553	0.945310000	0.993030000	Link
CVE-2023-6019	0.932040000	0.991500000	Link
CVE-2023-6018	0.911590000	0.989760000	Link
CVE-2023-52251	0.947690000	0.993370000	Link
CVE-2023-4966	0.970850000	0.998240000	Link
CVE-2023-49103	0.949290000	0.993590000	Link
CVE-2023-48795	0.962520000	0.995810000	Link
CVE-2023-47246	0.960640000	0.995470000	Link
CVE-2023-46805	0.962030000	0.995730000	Link
CVE-2023-46747	0.972980000	0.998990000	Link
CVE-2023-46604	0.970640000	0.998160000	Link
CVE-2023-4542	0.941060000	0.992510000	Link
CVE-2023-43208	0.974590000	0.999690000	Link
CVE-2023-43177	0.957850000	0.995010000	Link
CVE-2023-42793	0.970480000	0.998110000	Link
CVE-2023-41892	0.905460000	0.989320000	Link
CVE-2023-41265	0.920970000	0.990420000	Link
CVE-2023-38205	0.955500000	0.994620000	Link
CVE-2023-38203	0.964750000	0.996330000	Link
CVE-2023-38146	0.920950000	0.990420000	Link
CVE-2023-38035	0.974570000	0.999680000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.967260000	0.997050000	Link
CVE-2023-3519	0.965540000	0.996590000	Link
CVE-2023-35082	0.965310000	0.996540000	Link
CVE-2023-35078	0.967840000	0.997220000	Link
CVE-2023-34993	0.973050000	0.999020000	Link
CVE-2023-34634	0.923140000	0.990620000	Link
CVE-2023-34362	0.969990000	0.997930000	Link
CVE-2023-34039	0.944770000	0.992970000	Link
CVE-2023-3368	0.928640000	0.991140000	Link
CVE-2023-33246	0.971590000	0.998470000	Link
CVE-2023-32315	0.973480000	0.999180000	Link
CVE-2023-30625	0.953680000	0.994310000	Link
CVE-2023-30013	0.962230000	0.995750000	Link
CVE-2023-29300	0.967820000	0.997210000	Link
CVE-2023-29298	0.968120000	0.997320000	Link
CVE-2023-28432	0.921730000	0.990510000	Link
CVE-2023-28343	0.957970000	0.995040000	Link
CVE-2023-28121	0.929610000	0.991250000	Link
CVE-2023-27524	0.969670000	0.997790000	Link
CVE-2023-27372	0.973760000	0.999310000	Link
CVE-2023-27350	0.969490000	0.997720000	Link
CVE-2023-26469	0.955890000	0.994680000	Link
CVE-2023-26360	0.963280000	0.995980000	Link
CVE-2023-26035	0.969120000	0.997600000	Link
CVE-2023-25717	0.950620000	0.993760000	Link
CVE-2023-25194	0.965880000	0.996680000	Link
CVE-2023-2479	0.961940000	0.995710000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-24489	0.972720000	0.998880000	Link
CVE-2023-23752	0.949000000	0.993530000	Link
CVE-2023-23333	0.963480000	0.996040000	Link
CVE-2023-22527	0.970950000	0.998290000	Link
CVE-2023-22518	0.965000000	0.996410000	Link
CVE-2023-22515	0.973250000	0.999100000	Link
CVE-2023-21839	0.941470000	0.992560000	Link
CVE-2023-21554	0.952650000	0.994160000	Link
CVE-2023-20887	0.971130000	0.998330000	Link
CVE-2023-1698	0.916400000	0.990050000	Link
CVE-2023-1671	0.962340000	0.995790000	Link
CVE-2023-0669	0.971830000	0.998550000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 30 Oct 2024

[UPDATE] [hoch] IBM Tivoli Netcool/OMNibus: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in IBM Tivoli Netcool/OMNibus ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Wed, 30 Oct 2024

[NEU] [hoch] Mozilla 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, vertrauliche Informationen preiszugeben oder einen Cross-Site-Scripting-Angriff durchzuführen.

- [Link](#)

—

Wed, 30 Oct 2024

[NEU] [hoch] X.Org X11 und Xming: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in X.Org X11 und Xming ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu erzeugen oder beliebigen Code auszuführen.

- [Link](#)

—

Wed, 30 Oct 2024

[NEU] [hoch] ServiceNow Now Platform: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonym Angreifer kann eine Schwachstelle in ServiceNow Now Platform ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Wed, 30 Oct 2024

[NEU] [hoch] Autodesk AutoCAD: Mehrere Schwachstellen

Ein entfernter anonym Angreifer kann mehrere Schwachstellen in Autodesk AutoCAD ausnutzen, um beliebigen Code auszuführen, einen 'Denial of Service'-Zustand zu erzeugen, Dateien zu manipulieren oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Wed, 30 Oct 2024

[NEU] [hoch] Apple Safari: Mehrere Schwachstellen

Ein anonym Angreifer kann mehrere Schwachstellen in Apple Safari ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, Daten zu manipulieren oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Wed, 30 Oct 2024

[NEU] [hoch] Keycloak: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Keycloak ausnutzen, um Informationen offenzulegen.

- [Link](#)

—

Wed, 30 Oct 2024

[UPDATE] [hoch] Grafana: Schwachstelle ermöglicht Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Grafana ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Wed, 30 Oct 2024

[NEU] [hoch] Google Chrome: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, Dateien zu manipulieren oder beliebigen Code auszuführen.

- [Link](#)

—

Wed, 30 Oct 2024

[UPDATE] [kritisch] CyberPanel: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in CyberPanel ausnutzen, um beliebigen Programmcode mit root Rechten auszuführen.

- [Link](#)

—

Wed, 30 Oct 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

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

- [Link](#)

—

Wed, 30 Oct 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder einen 'Denial of Service'-Zustand zu verursachen.

- [Link](#)

—

Wed, 30 Oct 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um Sicherheitsvorkehrungen zu umgehen und um Dateien zu manipulieren.

- [Link](#)

—

Wed, 30 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](#)

—

Wed, 30 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](#)

—

Wed, 30 Oct 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, 30 Oct 2024

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

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Kubernetes im “ingress-nginx controller” ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Wed, 30 Oct 2024

[UPDATE] [hoch] Red Hat OpenShift: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Red Hat OpenShift ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Wed, 30 Oct 2024

[UPDATE] [hoch] pgAdmin: Schwachstelle ermöglicht Privilegieneskalation

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

- [Link](#)

—

Wed, 30 Oct 2024

[UPDATE] [hoch] GNOME: Mehrere Schwachstellen ermöglichen Codeausführung

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

- [Link](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
10/30/2024	[openSUSE 15 Security Update : go1.22-openssl (SUSE-SU-2024:3772-1)]	critical
10/30/2024	[RHEL 8 / 9 : OpenShift Container Platform 4.16.z (RHSA-2024:8418)]	critical
10/30/2024	[RHEL 9 : krb5 (RHSA-2024:8577)]	critical
10/30/2024	[Slackware Linux 15.0 / current mozilla-firefox Multiple Vulnerabilities (SSA:2024-304-02)]	critical
10/30/2024	[Slackware Linux 15.0 / current mozilla-thunderbird Multiple Vulnerabilities (SSA:2024-304-03)]	critical
10/29/2024	[Debian dla-3939 : python-git-doc - security update]	critical
10/29/2024	[Google Chrome < 130.0.6723.91 Multiple Vulnerabilities]	critical
10/29/2024	[Google Chrome < 130.0.6723.91 Multiple Vulnerabilities]	critical
10/29/2024	[Google Chrome < 130.0.6723.92 Multiple Vulnerabilities]	critical
10/29/2024	[RHEL 9 : webkit2gtk3 (RHSA-2024:8492)]	critical
10/29/2024	[RHEL 9 : webkit2gtk3 (RHSA-2024:8496)]	critical
10/29/2024	[RHEL 8 : grafana (RHSA-2024:8507)]	critical
10/29/2024	[Debian dsa-5800 : xnest - security update]	critical
10/30/2024	[RHEL 9 : pki-servlet-engine (RHSA-2024:8528)]	high
10/30/2024	[openSUSE 15 Security Update : openssl-3 (SUSE-SU-2024:3766-1)]	high
10/30/2024	[openSUSE 15 Security Update : openssl-1_1 (SUSE-SU-2024:3765-1)]	high
10/30/2024	[openSUSE 15 Security Update : go1.23-openssl (SUSE-SU-2024:3773-1)]	high
10/30/2024	[RHEL 9 : kernel (RHSA-2024:8613)]	high
10/30/2024	[RHEL 9 : kernel-rt (RHSA-2024:8614)]	high
10/30/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : X.Org X Server vulnerability (USN-7085-1)]	high

Datum	Schwachstelle	Bewertung
10/30/2024	[Ubuntu 16.04 LTS / 18.04 LTS : X.Org X Server vulnerability (USN-7085-2)]	high
10/30/2024	[FreeBSD : forgejo – multiple vulnerabilities (f07c8f87-8e65-11ef-81b8-659bf0027d16)]	high
10/30/2024	[F5 Networks BIG-IP : Diffie-Hellman key exchange protocol vulnerability (K000148343)]	high
10/30/2024	[Slackware Linux 15.0 / current xorg-server Vulnerability (SSA:2024-304-04)]	high
10/30/2024	[Slackware Linux 15.0 / current tigervnc Vulnerability (SSA:2024-304-01)]	high
10/29/2024	[Fortinet Fortigate Double free with double usage of json_object_put (FG-IR-23-195)]	high
10/29/2024	[Fortinet Fortigate ['CSRF'] (FG-IR-20-158)]	high
10/29/2024	[Fortinet FortiWeb Stack-based buffer overflow in command line interpreter (FG-IR-21-132)]	high
10/29/2024	[RHEL 7 : python3 (RHSA-2024:8490)]	high
10/29/2024	[RHEL 9 : pki-servlet-engine (RHSA-2024:8494)]	high
10/29/2024	[RHEL 7 : postgresql (RHSA-2024:8495)]	high
10/29/2024	[Debian dla-3940 : xdmx - security update]	high
10/29/2024	[IBM MQ 9.1 < 9.1.0.24 LTS / 9.2 < 9.2.0.28 LTS / 9.3 < 9.3.0.25 LTS / 9.3 < 9.4.1 CD / 9.4 < 9.4.0.6 LTS (7174362)]	high
10/29/2024	[IBM MQ 9.1 < 9.1.0.24 LTS / 9.2 < 9.2.0.28 LTS / 9.3 < 9.3.0.25 LTS / 9.3 < 9.4.1 CD / 9.4 < 9.4.0.6 LTS (7174363)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Wed, 30 Oct 2024

WordPress WP-Automatic SQL Injection

This Metasploit module exploits an unauthenticated SQL injection vulnerability in the WordPress wp-automatic plugin versions prior to 3.92.1 to achieve remote code execution. The vulnerability allows the attacker to inject and execute arbitrary SQL commands, which can be used to create a malicious administrator account. The password for the new account is hashed using MD5. Once the administrator account is created, the attacker can upload and execute a malicious plugin, leading to full control over the WordPress site.

- [Link](#)

—

” “Wed, 30 Oct 2024

ABB Cylon Aspect 3.08.01 jsonProxy.php Username Enumeration

ABB Cylon Aspect version 3.08.01 is vulnerable to username enumeration in the jsonProxy.php endpoint. An unauthenticated attacker can interact with the UserManager servlet to enumerate valid usernames on the system. Since jsonProxy.php proxies requests to internal services without requiring authentication, attackers can gain unauthorized insights into valid usernames.

- [Link](#)

—

” “Wed, 30 Oct 2024

ABB Cylon Aspect 3.08.01 jsonProxy.php Information Disclosure

ABB Cylon Aspect version 3.08.01 is vulnerable to unauthorized information disclosure in the jsonProxy.php endpoint. An unauthenticated attacker can retrieve sensitive system information, including system time, uptime, memory usage, and network load statistics. The jsonProxy.php endpoint proxies these requests to internal services without requiring authentication, allowing attackers to obtain detailed system status data, which could aid in further attacks by revealing operational characteristics and resource utilization.

- [Link](#)

—

” “Wed, 30 Oct 2024

ABB Cylon Aspect 3.08.01 jsonProxy.php Unauthenticated Remote SSH Service Control

ABB Cylon Aspect version 3.08.01 is vulnerable to unauthorized SSH service configuration changes via the jsonProxy.php endpoint. An unauthenticated attacker can enable or disable the SSH service on the server by accessing the FTControlServlet with the sshenable parameter. The jsonProxy.php script proxies requests to localhost without enforcing authentication, allowing attackers to modify SSH settings and potentially gain further unauthorized access to the system.

- [Link](#)

—

” “Wed, 30 Oct 2024

ABB Cylon Aspect 3.08.01 jsonProxy.php Denial Of Service

ABB Cylon Aspect version 3.08.01 is vulnerable to an unauthenticated denial of service attack in the

jsonProxy.php endpoint. An attacker can remotely restart the main Java server by accessing the FTControlServlet with the restart parameter. The endpoint proxies requests to localhost without requiring authentication, enabling attackers to disrupt system availability by repeatedly triggering server restarts.

- [Link](#)

” “Wed, 30 Oct 2024

ABB Cylon Aspect 3.08.01 jsonProxy.php Unauthenticated Project Download

ABB Cylon Aspect version 3.08.01 is vulnerable to an unauthorized project file disclosure in jsonProxy.php. An unauthenticated remote attacker can issue a GET request abusing the DownloadProject servlet to download sensitive project files. The jsonProxy.php script bypasses authentication by proxying requests to localhost (AspectFT Automation Application Server), granting remote attackers unauthorized access to internal Java servlets. This exposes potentially sensitive project data and configuration details without requiring authentication.

- [Link](#)

” “Wed, 30 Oct 2024

ABB Cylon Aspect 3.08.01 jsonProxy.php Servlet Inclusion Authentication Bypass

ABB Cylon Aspect version 3.08.01 is vulnerable to remote, arbitrary servlet inclusion. The jsonProxy.php endpoint allows unauthenticated remote attackers to access internal services by proxying requests to localhost. This results in an authentication bypass, enabling attackers to interact with multiple java servlets without authorization, potentially exposing sensitive system functions and information.

- [Link](#)

” “Wed, 30 Oct 2024

ABB Cylon Aspect 3.08.01 jsonProxy.php Unauthenticated Credential Disclosure

ABB Cylon Aspect version 3.08.01 allows an unauthenticated attacker to disclose credentials in plain-text.

- [Link](#)

” “Wed, 30 Oct 2024

ABB Cylon Aspect 3.08.01 jsonProxy.php Cross Site Scripting

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated reflected cross-site scripting vulnerability. Input passed to the GET parameters query and application is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML/JS code in a user's browser session in context of an affected site.

- [Link](#)

—

” “Tue, 29 Oct 2024

Xerox Printers Authenticated Remote Code Execution

Various Xerox printers, such as models EC80xx, AltaLink, VersaLink, and WorkCentre, suffer from an authenticated remote code execution vulnerability.

- [Link](#)

—

” “Tue, 29 Oct 2024

ABB Cylon Aspect 3.08.01 Active Debug Data Exposure

ABB Cylon Aspect version 3.08.01 is deployed to unauthorized actors with debugging code still enabled or active, which can create unintended entry points or expose sensitive information.

- [Link](#)

—

” “Tue, 29 Oct 2024

Booked Scheduler 2.8.5 Cross Site Scripting / Open Redirection

Booked Scheduler version 2.8.5 suffers from cross site scripting and open redirection vulnerabilities.

- [Link](#)

—

” “Tue, 29 Oct 2024

UP-RESULT PRO 1.0 SQL Injection

UP-RESULT PRO version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 28 Oct 2024

ABB Cylon Aspect 3.08.01 getApplicationNamesJS.php Building/Project Name Exposure

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated building/project name exposure vulnerability.

- [Link](#)

—

” “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

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](#)

—

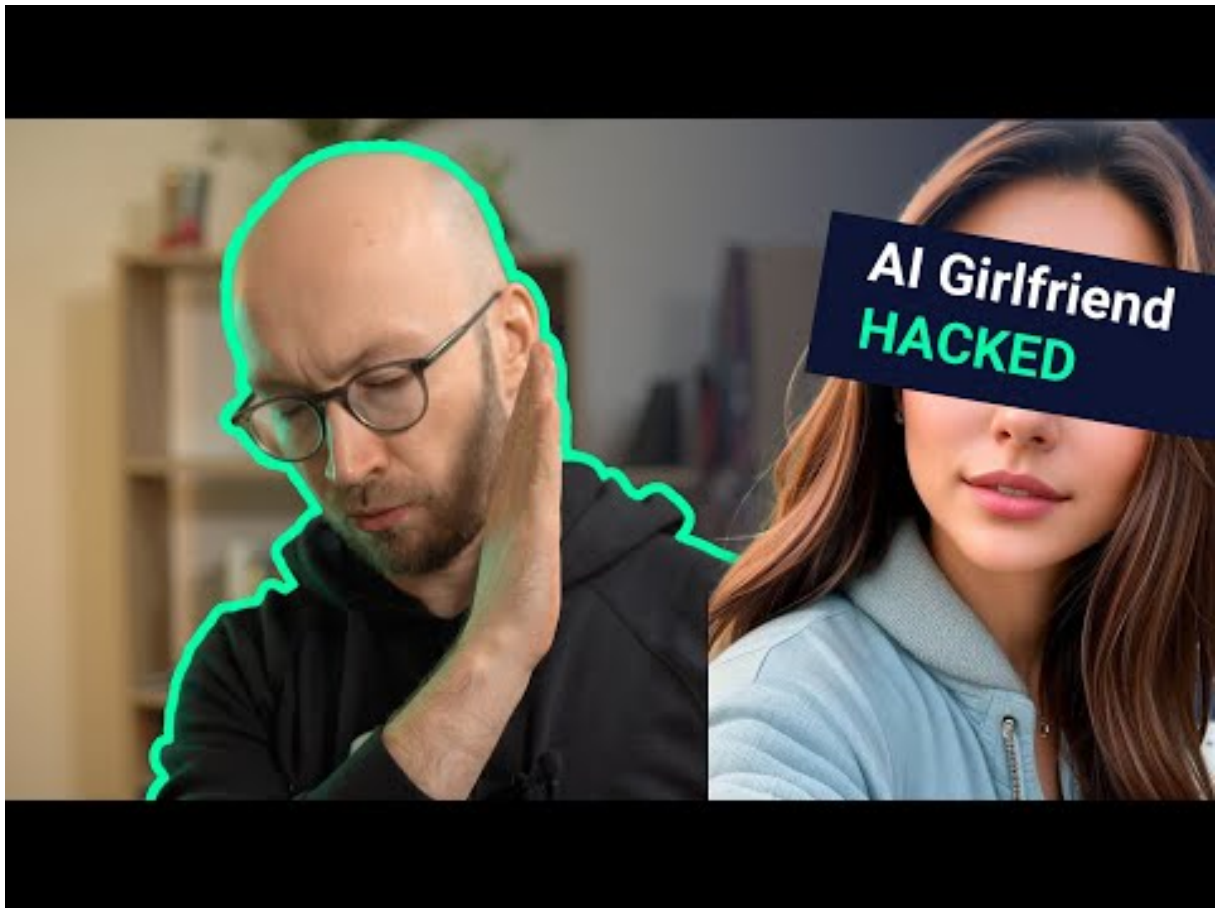
”

4.2 0-Days der letzten 5 Tage

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
2024-10-28	AEP	[DEU]	Link
2024-10-28	Blackburn College	[GBR]	Link
2024-10-27	Diocèse de St-Gall	[CHE]	Link
2024-10-26	Mairie du district 5 de Bucarest	[ROU]	Link
2024-10-26	Marysville Village Exempted Schools	[USA]	Link
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

Datum	Opfer	Land	Information
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
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

Datum	Opfer	Land	Information
2024-10-01	C.R. Laurence (CRL)	[USA]	Link

7 Ransomware-Erpressungen: (Okt)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-30	[illumin8global.com]	ransomhub	Link
2024-10-31	[TRANSAK]	stormous	Link
2024-10-30	[Maval Industries]	play	Link
2024-10-30	[Unlimited Lawn Care]	play	Link
2024-10-30	[Pureflow Airdog]	play	Link
2024-10-30	[iFocus Consulting]	play	Link
2024-10-30	[Pelsue]	play	Link
2024-10-30	[Paul White Company]	play	Link
2024-10-30	[Sunrise Express]	play	Link
2024-10-30	[PlayBoy]	playboy	Link
2024-10-30	[Jillamy (jillamy.com)]	fog	Link
2024-10-30	[IM Cannabis]	handala	Link
2024-10-30	[SmartSource (smartsource-inc.com)]	fog	Link
2024-10-30	[tlie.org]	ransomhub	Link
2024-10-30	[nagucoop.com]	ransomhub	Link
2024-10-29	[Spirit Lake Community School District]	medusa	Link
2024-10-24	[www.baymark.com]	ransomhub	Link
2024-10-29	[Astac]	play	Link
2024-10-29	[Dana Safety Supply]	play	Link
2024-10-29	[Dirksen Screw Products]	play	Link
2024-10-27	[noblehouse.com.ph]	ransomhub	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-29	[hcfinc.com]	ransomhub	Link
2024-10-29	[www.ztexconstruction.com]	ransomhub	Link
2024-10-29	[daserv.com]	blackbasta	Link
2024-10-29	[celo.com]	blackbasta	Link
2024-10-29	[CLAS Information Services]	bianlian	Link
2024-10-29	[rosenlegal.com]	blackbasta	Link
2024-10-29	[weberpackaging.com]	blackbasta	Link
2024-10-29	[Surfnet Communications]	arcusmedia	Link
2024-10-29	[anhf.org.auh]	abyss	Link
2024-10-29	[www.trinitesolutions.com]	apt73	Link
2024-10-29	[www.scopeset.de]	apt73	Link
2024-10-29	[sokkakreatif.com]	apt73	Link
2024-10-29	[www.legilog.fr]	apt73	Link
2024-10-29	[projektaip.ch]	abyss	Link
2024-10-29	[Jordan Public Schools (https://www.jordan.k12.mn.us/)]	fog	Link
2024-10-29	[Sage Automotive Interior (sageautomotiveinteriors.com)]	fog	Link
2024-10-29	[nathcompanies.com]	blacksuit	Link
2024-10-29	[Berridge Manufacturing Co.]	BrainCipher	Link
2024-10-25	[Mastery Schools]	dragonforce	Link
2024-10-25	[Accuracy International]	dragonforce	Link
2024-10-28	[K&S Tool & Mfg Co.]	BrainCipher	Link
2024-10-28	[Basilio Advogados]	BrainCipher	Link
2024-10-28	[CHRISTODOULOS G. VASSILIADES & CO. LLC]	BrainCipher	Link
2024-10-28	[Fortis]	killsec	Link
2024-10-28	[phxcmp.com]	ELDorado	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-28	[barranquitas.pr.gov]	ElDorado	Link
2024-10-28	[www.keizers.ca]	ElDorado	Link
2024-10-28	[mmpunion.com]	ElDorado	Link
2024-10-28	[German Chamber of Commerce]	playboy	Link
2024-10-26	[flueid.com]	ransomhub	Link
2024-10-03	[guymontigers.com]	ransomhub	Link
2024-10-28	[harrispersonalinjury.com]	ransomhub	Link
2024-10-25	[Evergreen SD50 (evergreensd50.com)]	fog	Link
2024-10-28	[ConCash]	killsec	Link
2024-10-28	[AGAS]	handala	Link
2024-10-16	[Drogarias Preço Bom]	apos	Link
2024-10-25	[Lakesight Technologies Information]	medusa	Link
2024-10-25	[Island Coastal Services Ltd]	medusa	Link
2024-10-27	[Mixfame]	killsec	Link
2024-10-27	[payxpress.co.il]	ransomhub	Link
2024-10-27	[Texas Tech University Health Sciences Center]	interlock	Link
2024-10-22	[melangesystems.com]	ransomhub	Link
2024-10-24	[mkarrari.com.br]	ransomhub	Link
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

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-26	[Bliss Worldwide]	killsec	Link
2024-10-05	[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	[hcsghcorp.com]	underground	Link
2024-10-25	[SRS-Stahl GmbH]	sarcoma	Link
2024-10-25	[MESHWORKS]	sarcoma	Link
2024-10-25	[De Rose Lawyers]	rhapsida	Link
2024-10-25	[Matouk Bassiouny]	raworld	Link
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[nracs.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
2024-10-11	[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
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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
2024-10-21	[Precision Steel Services]	spacebears	Link
2024-10-22	[tkg.com]	ransomhub	Link
2024-10-22	[lpahorticole.faylbilot.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

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-22	[American Mechanical, inc]	medusa	Link
2024-10-22	[American Medical Billing]	medusa	Link
2024-10-08	[mauguio-carnon.com]	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
2024-10-03	[milleredge.com]	blackbasta	Link
2024-10-08	[gkcorp.com]	blackbasta	Link
2024-10-02	[ssbwc.com]	blackbasta	Link
2024-10-03	[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
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	[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	[Interbel]	arcusmedia	Link
2024-10-20	[Petropolis Pet Resort]	arcusmedia	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
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
2024-10-12	[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
2024-10-19	[SPECTRUMCHEMICAL.COM]	clop	Link
2024-10-19	[clinicia.com]	ransomhub	Link
2024-10-16	[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

Datum	Opfer	Ransomware-Gruppe	Webseite
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
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.aristoicclassical.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?!?????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

Datum	Opfer	Ransomware-Gruppe	Webseite
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
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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
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
2024-10-01	[gfm-uk.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

Datum	Opfer	Ransomware-Gruppe	Webseite
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
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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]	clap	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
2024-10-04	[Pete's Road Service]	play	Link
2024-10-03	[release.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

Datum	Opfer	Ransomware-Gruppe	Webseite
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
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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.