Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241019

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 **13**
4.1 Exploits der letzten 5 Tage . . . 13
4.2 0-Days der letzten 5 Tage . . . 17

5 Die Hacks der Woche **23**
5.0.1 AI Girlfriends HACKED (Da steht uns noch was bevor) . . . 23

6 Cyberangriffe: (Okt) **24**

7 Ransomware-Erpressungen: (Okt) **25**

8 Quellen **35**
8.1 Quellenverzeichnis . . . 35

9 Impressum **36**

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

Kritische Sicherheitslücke: Angreifer können Kubernetes als Root attackieren

Bestimmte Kubernetes Image Builder erzeugen VM-Images mit statischen Zugangsdaten. Admins müssen bestehende Images neu erstellen.

- Link

—

Oracle schützt Softwareprodukte mit 334 Sicherheitsupdates

Mit seinen quartalsweise erscheinenden Sicherheitsupdates sichert Oracle abermals das eigene Softwareportfolio ab.

- Link

—

Sicherheitsupdates: Root-Attacken auf VoIP-Adapter von Cisco möglich

Angreifer können mehrere Produkte von Cisco attackieren und im schlimmsten Fall Systeme kompromittieren.

- Link

—

F5 BIG-IP: Zugriffsbeschränkungen umgehbar

F5 hat eine Sicherheitslücke in der Monitor-Funktion von BIG-IP gemeldet. Angreifer können betroffene Systeme kompromittieren.

- Link

—

Solarwinds: Lücken in Plattform und Serv-U ermöglichen Schadcode-Schmuggel

Solarwinds warnt vor Sicherheitslücken in der Plattform und in Serv-U. Angreifer können etwa Code einschleusen oder ihre Rechte ausweiten.

- Link

—

VMware HCX: Codeschmuggel durch SQL-Injection-Lücke möglich

Broadcom hat mit einem Update eine Sicherheitslücke in VMware HCX geschlossen. Angreifer können durch sie Code einschleusen und ausführen.

- Link

—

Sicherheitsupdate: Zwei Drucker-Modelle aus HPs DesignJet-Serie attackierbar

Setzen Angreifer erfolgreich an einer Sicherheitslücke in bestimmten HP-Druckern an, können sie eigentlich abgeschottete Informationen einsehen.

- Link

—

Jetzt patchen! Angreifer attackieren Solarwinds Web Help Desk

Derzeit laufen Attacken auf die Kundensupport-Software Web Help Desk von Solarwinds. Sicherheitsupdates stehen zum Download.

- Link

—

Github Enterprise Server: Angreifer können Authentifizierung umgehen

Unter bestimmten Voraussetzungen sind unbefugte Zugriffe auf Github Enterprise Server möglich. Sicherheitsupdates sind verfügbar.

- Link

—

Kritische Sicherheitslücken: Telerik Report Server auf mehreren Wegen angreifbar

Das Business-Reportingtool Telerik Report Server ist verwundbar. Patches schließen unter anderem eine Schadcodelücke.

- 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	0.994910000	Link
CVE-2023-6895	0.925010000	0.990750000	Link
CVE-2023-6553	0.948430000	0.993400000	Link
CVE-2023-6019	0.933700000	0.991590000	Link
CVE-2023-6018	0.911590000	0.989650000	Link
CVE-2023-52251	0.948240000	0.993380000	Link
CVE-2023-4966	0.971220000	0.998370000	Link
CVE-2023-49103	0.947620000	0.993270000	Link
CVE-2023-48795	0.965360000	0.996540000	Link
CVE-2023-47246	0.960640000	0.995410000	Link
CVE-2023-46805	0.961520000	0.995580000	Link
CVE-2023-46747	0.971910000	0.998570000	Link
CVE-2023-46604	0.971080000	0.998310000	Link
CVE-2023-4542	0.941060000	0.992420000	Link
CVE-2023-43208	0.974200000	0.999510000	Link
CVE-2023-43177	0.954040000	0.994310000	Link
CVE-2023-42793	0.970970000	0.998270000	Link
CVE-2023-41892	0.905460000	0.989200000	Link
CVE-2023-41265	0.920970000	0.990320000	Link
CVE-2023-39143	0.905600000	0.989210000	Link
CVE-2023-38205	0.954790000	0.994420000	Link
CVE-2023-38203	0.964750000	0.996320000	Link
CVE-2023-38146	0.920950000	0.990310000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-38035	0.974710000	0.999740000	Link
CVE-2023-36845	0.967920000	0.997250000	Link
CVE-2023-3519	0.964810000	0.996330000	Link
CVE-2023-35082	0.967900000	0.997240000	Link
CVE-2023-35078	0.967840000	0.997200000	Link
CVE-2023-34993	0.973050000	0.999010000	Link
CVE-2023-34634	0.923140000	0.990540000	Link
CVE-2023-34362	0.970450000	0.998060000	Link
CVE-2023-34105	0.927500000	0.990970000	Link
CVE-2023-34039	0.941110000	0.992430000	Link
CVE-2023-3368	0.937940000	0.992070000	Link
CVE-2023-33246	0.970550000	0.998110000	Link
CVE-2023-32315	0.973230000	0.999090000	Link
CVE-2023-30625	0.953820000	0.994270000	Link
CVE-2023-30013	0.962230000	0.995730000	Link
CVE-2023-29300	0.967820000	0.997200000	Link
CVE-2023-29298	0.969430000	0.997660000	Link
CVE-2023-28432	0.921730000	0.990410000	Link
CVE-2023-28343	0.957650000	0.994920000	Link
CVE-2023-28121	0.922260000	0.990450000	Link
CVE-2023-27524	0.969670000	0.997750000	Link
CVE-2023-27372	0.973980000	0.999410000	Link
CVE-2023-27350	0.968980000	0.997520000	Link
CVE-2023-26469	0.955890000	0.994630000	Link
CVE-2023-26360	0.963280000	0.995940000	Link
CVE-2023-26035	0.967750000	0.997170000	Link
CVE-2023-25717	0.950620000	0.993710000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-25194	0.966130000	0.996720000	Link
CVE-2023-2479	0.961840000	0.995660000	Link
CVE-2023-24489	0.972860000	0.998930000	Link
CVE-2023-23752	0.949000000	0.993480000	Link
CVE-2023-23333	0.960430000	0.995350000	Link
CVE-2023-22527	0.970410000	0.998040000	Link
CVE-2023-22518	0.962690000	0.995810000	Link
CVE-2023-22515	0.973650000	0.999250000	Link
CVE-2023-21839	0.941470000	0.992470000	Link
CVE-2023-21554	0.952650000	0.994080000	Link
CVE-2023-20887	0.970950000	0.998260000	Link
CVE-2023-1698	0.923310000	0.990580000	Link
CVE-2023-1671	0.962220000	0.995720000	Link
CVE-2023-0669	0.971830000	0.998540000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 18 Oct 2024

[NEU] [hoch] Bitdefender Total Security: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen

Ein Angreifer aus einem angrenzenden Netzwerk kann mehrere Schwachstellen in Bitdefender Total Security ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Fri, 18 Oct 2024

[UPDATE] [hoch] Cisco Analog Telephone Adaptor (ATA): Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen im Cisco Analog Telephone Adaptor ATA 191 und ATA 192 ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Cross-Site-Scripting-Angriff durchzuführen oder einen Denial-of-

Service-Zustand zu erzeugen.
- Link

—

Fri, 18 Oct 2024

[NEU] [UNGEPATCHT] [hoch] D-LINK Router: Mehrere Schwachstellen ermöglichen Codeausführung

Ein Angreifer aus einem angrenzenden Netzwerk kann mehrere Schwachstelle in D-LINK Router ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Fri, 18 Oct 2024

[NEU] [hoch] Grafana: Schwachstelle ermöglicht Codeausführung

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

—

Fri, 18 Oct 2024

[UPDATE] [hoch] International Components for Unicode (ICU): Schwachstelle ermöglichen Ausführen von beliebigem Programmcode mit Benutzerrechten

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in der Bibliothek ICU ausnutzen, um beliebigen Programmcode mit Benutzerrechten auszuführen.
- Link

—

Fri, 18 Oct 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Schwachstelle ermöglicht Codeausführung

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

—

Fri, 18 Oct 2024

[UPDATE] [hoch] Intel PROSet Wireless WiFi Software: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Intel PROSet Wireless WiFi Software ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Fri, 18 Oct 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um

vertrauliche Informationen offenzulegen oder einen nicht näher spezifizierten Angriff zu starten.
- Link

—

Fri, 18 Oct 2024

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

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

—

Fri, 18 Oct 2024

[UPDATE] [hoch] Oracle Construction and Engineering: Mehrere Schwachstellen

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Oracle Construction and Engineering ausnutzen, um die Vertraulichkeit und Integrität zu gefährden.
- Link

—

Fri, 18 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, 18 Oct 2024

[UPDATE] [kritisch] Veeam Backup & Replication: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Veeam Backup & Replication ausnutzen, um Dateien zu manipulieren, erweiterte Rechte zu erlangen, beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen und vertrauliche Informationen preiszugeben.
- Link

—

Fri, 18 Oct 2024

[UPDATE] [hoch] CUPS: Mehrere Schwachstellen ermöglichen Ausführung von beliebigem Programmcode

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in CUPS ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen und um Informationen offenzulegen.
- Link

—

Fri, 18 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, 18 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, 18 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

—

Fri, 18 Oct 2024

[UPDATE] [hoch] Google Chrome / Mmicrosoft Edge: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

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

- Link

—

Thu, 17 Oct 2024

[NEU] [UNGEPATCHT] [hoch] OpenSSL: Schwachstelle ermöglicht Denial of Service und Remote-Code-Ausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in OpenSSL ausnutzen, um einen Denial of Service Angriff durchzuführen oder um beliebigen Code auszuführen.

- Link

—

Thu, 17 Oct 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service zu verursachen.

- Link

—

Thu, 17 Oct 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen ermöglichen Manipulation von Dateien

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um Dateien zu manipulieren.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
10/18/2024	[Oracle Database Server (October 2024 CPU)]	critical
10/18/2024	[Docker for Windows < 4.34.3 RCE]	critical
10/18/2024	[Docker Desktop < 4.34.3 RCE (macOS)]	critical
10/18/2024	[Docker Desktop < 4.34.3 RCE]	critical
10/18/2024	[SUSE SLES15 Security Update : kernel (Live Patch 14 for SLE 15 SP5) (SUSE-SU-2024:3710-1)]	high
10/18/2024	[SUSE SLES15 Security Update : kernel (Live Patch 2 for SLE 15 SP6) (SUSE-SU-2024:3708-1)]	high
10/18/2024	[SUSE SLES15 Security Update : kernel (Live Patch 46 for SLE 15 SP3) (SUSE-SU-2024:3704-1)]	high
10/18/2024	[SUSE SLES15 Security Update : kernel (Live Patch 28 for SLE 15 SP4) (SUSE-SU-2024:3707-1)]	high
10/18/2024	[SUSE SLES15 Security Update : kernel (Live Patch 18 for SLE 15 SP4) (SUSE-SU-2024:3706-1)]	high
10/18/2024	[Photon OS 4.0: Wireshark PHSA-2024-4.0-0702]	high
10/18/2024	[Juniper Junos OS DoS (JSA88102)]	high
10/18/2024	[Foxit PDF Editor for Mac < 12.1.6 Multiple Vulnerabilities]	high

Datum	Schwachstelle	Bewertung
10/18/2024	[Foxit PDF Editor for Mac < 11.1.10 Multiple Vulnerabilities]	high
10/18/2024	[Foxit PDF Editor < 11.2.11 Multiple Vulnerabilities]	high
10/18/2024	[Oracle HTTP Server (October 2024 CPU)]	high
10/18/2024	[Palo Alto Networks Expedition Command Injection (CVE-2024-9463)]	high
10/18/2024	[Oracle Java SE Multiple Vulnerabilities (October 2024 CPU)]	high
10/18/2024	[Palo Alto GlobalProtect Agent Local Privilege Escalation (CVE-2024-9473)]	high
10/18/2024	[AlmaLinux 9 : java-11-openjdk (ALSA-2024:8121)]	high
10/18/2024	[AlmaLinux 9 : webkit2gtk3 (ALSA-2024:8180)]	high
10/18/2024	[AlmaLinux 9 : java-21-openjdk (ALSA-2024:8127)]	high
10/18/2024	[AlmaLinux 9 : java-1.8.0-openjdk (ALSA-2024:8117)]	high
10/18/2024	[AlmaLinux 9 : java-17-openjdk (ALSA-2024:8124)]	high
10/18/2024	[Autodesk Revit 2024.x < 2024.2.2 / 2025.x < 2025.3 PDF File Parsing Out-of-Bounds Write (ADSK-SA-2024-0018)]	high
10/18/2024	[Autodesk Revit 2024.x < 2024.3 / 2025.x < 2025.3 RFA File Parsing Buffer Overflow (ADSK-SA-2024-0017)]	high
10/18/2024	[FreeBSD : electron{31,32} – multiple vulnerabilities (815bf172-ab9e-4c4b-9662-d18b0054330d)]	high
10/18/2024	[Mattermost Server 9.5.x < 9.5.8 / 9.8.x < 9.8.3 / 9.9.x < 9.9.2 / 9.10.x < 9.10.1 (MMSA-2024-00368)]	high
10/18/2024	[Mattermost Server 9.5.x < 9.5.8 / 9.8.x < 9.8.3 / 9.9.x < 9.9.2 / 9.10.x < 9.10.1 (MMSA-2024-00374)]	high
10/18/2024	[Oracle Linux 8 / 9 : java-17-openjdk (ELSA-2024-8124)]	high
10/18/2024	[Oracle Linux 8 / 9 : java-1.8.0-openjdk (ELSA-2024-8117)]	high
10/18/2024	[actionmailer Ruby Library 3.x < 6.1.7.9 / 7.0.x < 7.0.8.5 / 7.1.x < 7.1.4.1 / 7.2.x < 7.2.1.1 DoS (CVE-2024-47889)]	high
10/18/2024	[CBL Mariner 2.0 Security Update: libarchive (CVE-2024-48958)]	high

Datum	Schwachstelle	Bewertung
10/18/2024	[CBL Mariner 2.0 Security Update: libarchive (CVE-2024-48957)]	high
10/17/2024	[Teltonika Remote Management System and RUT Model Routers External Control of System or Configuration Setting (CVE-2023-32349)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“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

—

” “Mon, 14 Oct 2024

ABB Cylon Aspect 3.08.00 yumSettings.php Command Injection

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 PROXY HTTP POST parameter called by the yumSettings.php script.

- Link

—

” “Mon, 14 Oct 2024

Vivo Fibra Askey RTF8225VW Command Execution

The Vivo Fibra Askey RTF8225VW modem suffers from an input validation vulnerability that allows for full escalation to a functioning shell once logged in and using the restricted aspsh shell.

- Link

—

” “Mon, 14 Oct 2024

WordPress File Manager Advanced Shortcode 2.3.2 Code Injectin / Shell Upload

WordPress File Manager Advanced Shortcode plugin version 2.3.2 suffers from a code injection vulnerability that allows for remote shell upload.

- Link

—

” “Mon, 14 Oct 2024

TOTOLINK 9.x Command Injection

TOTOLINK version 9.x suffers from a remote command injection vulnerability.

- Link

—

” “Mon, 14 Oct 2024

MagnusBilling 7.x Command Injection

MagnusBilling version 7.x suffers from a remote command injection vulnerability.

- Link

—

” “Mon, 14 Oct 2024

Bookstore Management System 1.0 SQL Injection

Bookstore Management System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Mon, 14 Oct 2024

Peel Shopping 2.x Cross Site Scripting / SQL Injection

Peel Shopping versions 2.x and below 3.1 suffer from cross site scripting and remote SQL injection vulnerabilities. This was already noted discovery in 2012 by Cyber-Crystal but this data provides more details.

- Link

—

” “Fri, 11 Oct 2024

ABB Cylon Aspect 3.07.02 user.properties Default Credentials

ABB Cylon Aspect version 3.07.02 uses a weak set of default administrative credentials that can be guessed in remote password attacks and used to gain full control of the system.

- Link

—

” “Fri, 11 Oct 2024

ABB Cylon Aspect 3.08.00 dialupSwitch.php Remote Code 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 MODEM HTTP POST parameter called by the dialupSwitch.php script.

- Link

—

” “Fri, 11 Oct 2024

ABB Cylon Aspect 3.07.02 sshUpdate.php Unauthenticated Remote SSH Service Control

ABB Cylon Aspect version 3.07.02 suffers from a vulnerability that allows an unauthenticated attacker to enable or disable the SSH daemon by sending a POST request to sshUpdate.php with a simple JSON payload. This can be exploited to start the SSH service on the remote host without proper authentication, potentially enabling unauthorized access or stop and deny service access.

- Link

—

” “Fri, 11 Oct 2024

TerraMaster TOS 4.2.29 Code Injection / Local File Inclusion

TerraMaster TOS version 4.2.29 suffers from a remote code injection vulnerability leveraging a local file inclusion vulnerability.

- Link

—

” “Fri, 11 Oct 2024

SolarView Compact 6.00 Code Injection

SolarView Compact version 6.00 suffers from a PHP code injection vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Fri, 18 Oct 2024

ZDI-24-1420: Schneider Electric EcoStruxure Data Center Expert XML External Entity Processing Information Disclosure Vulnerability

- Link

—

” “Thu, 17 Oct 2024

ZDI-24-1419: Trend Micro Deep Security Improper Access Control Local Privilege Escalation Vul-

nerability

- Link

—

” “Thu, 17 Oct 2024

ZDI-24-1418: Trend Micro Cloud Edge REST API Command Injection Remote Code Execution Vulnerability

- Link

—

” “Thu, 17 Oct 2024

ZDI-24-1417: Schneider Electric EcoStruxure Data Center Expert Improper Verification of Cryptographic Signature Remote Code Execution Vulnerability

- Link

—

” “Thu, 17 Oct 2024

ZDI-24-1416: Schneider Electric EcoStruxure Data Center Expert Missing Authentication Information Disclosure Vulnerability

- Link

—

” “Thu, 17 Oct 2024

ZDI-24-1415: Schneider Electric Zelio Soft 2 ZM2 File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 17 Oct 2024

ZDI-24-1414: Oracle VirtualBox BusLogic Uninitialized Memory Information Disclosure Vulnerability

- Link

—

” “Thu, 17 Oct 2024

ZDI-24-1413: Oracle VirtualBox TPM Heap-based Buffer Overflow Local Privilege Escalation Vulnerability

- Link

—

” “Thu, 17 Oct 2024

ZDI-24-1412: Oracle VirtualBox Shared Folders Incorrect Authorization Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1411: Delta Electronics CNCSoft-G2 DPAX File Parsing Uninitialized Variable Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1410: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1409: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1408: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1407: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1406: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1405: Delta Electronics CNCSoft-G2 ALM File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1404: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1403: Delta Electronics CNCSoft-G2 DPAX File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1402: Delta Electronics CNCSoft-G2 DOPSoft DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1401: Delta Electronics CNCSoft-G2 DOPSoft DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1400: Delta Electronics CNCSoft-G2 DPAX File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1399: Delta Electronics CNCSoft-G2 DPAX File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1398: Delta Electronics CNCSoft-G2 DOPSoft ALM File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1397: Delta Electronics CNCSoft-G2 DOPSoft CMT File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1396: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1395: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1394: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1393: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1392: Delta Electronics CNCSoft-G2 DPAX File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1391: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1390: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1389: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1388: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1387: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1386: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1385: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1384: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1383: PostHog database_schema Server-Side Request Forgery Information Disclosure Vulnerability

- Link

—

” “Tue, 15 Oct 2024

ZDI-24-1382: QEMU SCSI Use-After-Free Local Privilege Escalation Vulnerability

- Link

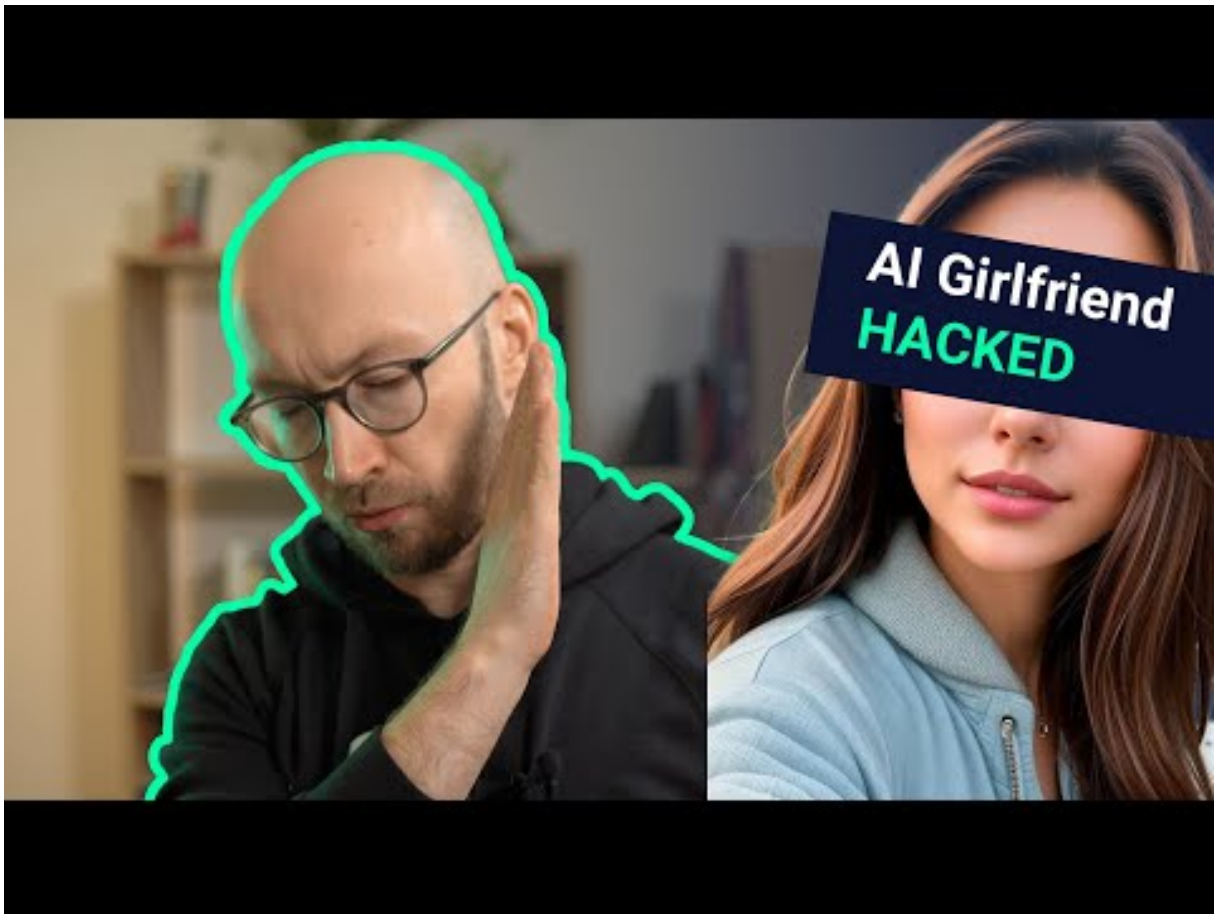
—

”

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
2024-10-17	Formpipe	[DNK]	Link
2024-10-15	aap Implantate AG	[DEU]	Link
2024-10-15	Comune di Aversa	[ITA]	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
2024-10-13	Johannesstift-Diakonie Berlin	[DEU]	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

Datum	Opfer	Land	Information
2024-10-02	Wayne County	[USA]	Link
2024-10-02	Traffics GmbH	[DEU]	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
2024-10-19	[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
2024-10-18	[INDIBA Group]	cicada3301	Link
2024-10-16	[Astolabs.com]	ransomhub	Link
2024-10-18	[Neighbors Credit Union]	blacksuit	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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-10-14	[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	[confidencegroup.com.bd]	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	[Volta River Authority]	blacksuit	Link
2024-10-11	[Protective Industrial Products]	hunters	Link
2024-10-11	[Therabel Lucien Pharma SAS]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-10-07	[trulysmall.com]	ransomhub	Link
2024-10-07	[nspproteins.com]	ransomhub	Link
2024-10-07	[Richmond Auto Mall - Full Leak]	monti	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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-10-04	[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	[GenPro Inc.]	blacksuit	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

Datum	Opfer	Ransomware-Grupppe	Webseite
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	[rollxvans.com]	ransomhub	Link
2024-10-02	[ETC Companies]	akira	Link
2024-10-02	[Branhaven Chrysler Dodge Jeep Ram]	blacksuit	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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.