Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241012

Inhaltsverzeichnis

1 Editorial

Guten Morgen,

willkommen zum Cybersecurity Morgenreport von Cyberwald, Ihrem täglichen Begleiter in der Welt der IT-Sicherheit. Als nicht-kommerzielles Projekt ist es unser Anliegen, Awareness und Wissen rund um das Thema Cybersecurity kostenlos zu vermitteln. In der heutigen digitalen Welt ist es für Unternehmen von entscheidender Bedeutung, sich über aktuelle Sicherheitsrisiken zeitnah zu informieren. Cyberbedrohungen entwickeln sich ständig weiter und können erhebliche Schäden verursachen, wenn sie nicht rechtzeitig erkannt und abgewehrt werden. Durch die Nutzung aktueller Informationen können Unternehmen ihre IT-Sicherheitsmaßnahmen stärken und sich effektiv gegen diese Bedrohungen schützen.

Unser Ziel ist es, Ihnen, den IT-Verantwortlichen, einen kompakten und leicht verständlichen Überblick über aktuelle Sicherheitsrisiken zu geben. Wir präsentieren Ihnen täglich Sicherheitsmeldungen und Berichte über neue Sicherheitslücken, die Ihre Systeme und Daten bedrohen könnten.

Darüber hinaus listen wir aktuelle Cyberangriffe und Ransomware-Vorfälle auf. Dies ist von besonderer Bedeutung, da es Unternehmen ermöglicht, sich auf mögliche Supply-Chain- und Phishing-Angriffe vorzubereiten. Durch das Verständnis der Methoden und Taktiken, die von Cyberkriminellen verwendet werden, können Unternehmen ihre Verteidigungsmaßnahmen entsprechend anpassen und stärken.

Für den Cybersecurity Morgenreport greifen wir automatisiert auf öffentliche Informationsquellen zu, filtern und sortieren diese Informationen, um sie Ihnen in einer übersichtlichen Form zur Verfügung zu stellen. Wir bemühen uns, die Inhalte so verständlich wie möglich zu gestalten und vorzugsweise vollständig in deutscher Sprache wiederzugeben. Bei Bedarf übersetzen wir die öffentlichen Informationen und fassen sie durch eine KI zusammen.

Der Cybersecurity Morgenreport ist ein dynamisches Projekt. Wir passen und erweitern unsere Inhalte ständig, um Ihnen die relevantesten und aktuellsten Informationen zu liefern. Derzeit befinden wir uns im Alpha-Stadium des Projekts und freuen uns über Ihr Feedback und Ihre Anregungen.

Wir hoffen, dass der Cybersecurity Morgenreport Ihnen hilft, Ihre IT-Sicherheitsmaßnahmen zu verbessern und Ihre Systeme vor den ständig wechselnden Bedrohungen zu schützen. Bleiben Sie sicher und informiert mit dem Cybersecurity Morgenreport von Cyberwald.

Ihr Cyberwald-Team

2 Security-News

2.1 Heise - Security-Alert

CISA warnt vor Sicherheitslücken in 21 IoT-Industrie-Kontrollsystemen

Die US-IT-Sicherheitsbehörde CISA hat 21 Sicherheitsmeldungen zu industriellen Steuerungssystemen veröffentlicht. IT-Verantwortliche sollten sie prüfen.

- Link

—

Anonymisierendes Linux: Tails 6.8.1 kann persistenten Speicher reparieren

Das zum anonymen Surfen gedachte Tails-Linux schließt in Version 6.8.1 eine Sicherheitslücke. Es verbessert zudem den Umgang mit persistentem Speicher.

- Link

—

Juniper: Mehr als 30 Sicherheitslücken gestopft

Juniper Networks hat mehr als 30 Sicherheitsmitteilungen veröffentlicht. Zugehörige Updates schließen Schwachstellen in Junos OS.

- Link

—

Firefox- und Thunderbird-Notfall-Update stopft angegriffenes Sicherheitsleck

Neue Versionen von Firefox und Thunderbird schließen Sicherheitslücken, die bereits in freier Wildbahn angegriffen werden.

- Link

—

Kritische Fortinet-Sicherheitslücke wird angegriffen

Die US-amerikanische IT-Sicherheitsbehörde CISA warnt, dass eine ältere Lücke in Fortinet-Produkten aktuell angegriffen wird.

- Link

—

HP Business-Notebooks: Hotkey-Unterstützung ermöglicht Rechteausweitung

Hewlett Packard warnt vor einer Schwachstelle im Hotkey-Support von Business-Notebooks. Angreifer können dadurch ihre Rechte ausweiten.

- Link

—

Wordpress-Plug-in: Abermals gravierende Sicherheitslücke in Litespeed Cache

Auf mehr als sechs Millionen Websites lauert eine schwerwiegende Schwachstelle im Wordpress-Plug-in Litespeed Cache. Ein Update steht bereit.

- Link

—

Ivanti stopft ausgenutzte Sicherheitslücken und mehr

Ivanti aktualisiert mehrere Software-Pakete. Darunter CSA, die bereits attackiert wird, oder Connect Secure mit kritischen Lecks.

- Link

—

Adobe-Patchday: Neun Produkte mit Sicherheitslücken

Adobe hat zum Oktober-Patchday Sicherheitsupdates für neun Produkte veröffentlicht. Admins sollten sie zügig installieren.

- Link

—

Microsoft Patchday: Zwei Zeroday-Lücken werden bereits angegriffen

Zum Microsoft-Patchday im Oktober dichten die Entwickler auch zwei Sicherheitslücken ab, die bereits in freier Wildbahn angegriffen werden.

- 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	0.994880000	Link
CVE-2023-6895	0.927330000	0.990890000	Link
CVE-2023-6553	0.948430000	0.993360000	Link
CVE-2023-6019	0.933510000	0.991510000	Link
CVE-2023-52251	0.949200000	0.993480000	Link
CVE-2023-4966	0.970840000	0.998210000	Link
CVE-2023-49103	0.947620000	0.993250000	Link
CVE-2023-48795	0.964670000	0.996260000	Link
CVE-2023-47246	0.960640000	0.995380000	Link
CVE-2023-46805	0.960890000	0.995430000	Link
CVE-2023-46747	0.971910000	0.998560000	Link
CVE-2023-46604	0.971080000	0.998310000	Link
CVE-2023-4542	0.941060000	0.992370000	Link
CVE-2023-43208	0.974200000	0.999510000	Link
CVE-2023-43177	0.954700000	0.994420000	Link
CVE-2023-42793	0.970970000	0.998270000	Link
CVE-2023-41892	0.904950000	0.989140000	Link
CVE-2023-41265	0.907590000	0.989320000	Link
CVE-2023-39143	0.940700000	0.992320000	Link
CVE-2023-38205	0.951890000	0.993920000	Link
CVE-2023-38203	0.964750000	0.996310000	Link
CVE-2023-38146	0.919150000	0.990100000	Link
CVE-2023-38035	0.974600000	0.999680000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.967920000	0.997220000	Link
CVE-2023-3519	0.964810000	0.996320000	Link
CVE-2023-35082	0.967900000	0.997210000	Link
CVE-2023-35078	0.969440000	0.997640000	Link
CVE-2023-34993	0.973450000	0.999170000	Link
CVE-2023-34634	0.923140000	0.990490000	Link
CVE-2023-34362	0.970450000	0.998050000	Link
CVE-2023-34105	0.927500000	0.990920000	Link
CVE-2023-34039	0.943770000	0.992690000	Link
CVE-2023-3368	0.934610000	0.991630000	Link
CVE-2023-33246	0.970550000	0.998090000	Link
CVE-2023-32315	0.973230000	0.999090000	Link
CVE-2023-30625	0.953820000	0.994270000	Link
CVE-2023-30013	0.965950000	0.996660000	Link
CVE-2023-29300	0.967820000	0.997170000	Link
CVE-2023-29298	0.969430000	0.997640000	Link
CVE-2023-28432	0.921930000	0.990370000	Link
CVE-2023-28343	0.957650000	0.994890000	Link
CVE-2023-28121	0.922260000	0.990400000	Link
CVE-2023-27524	0.969670000	0.997720000	Link
CVE-2023-27372	0.973980000	0.999420000	Link
CVE-2023-27350	0.968980000	0.997500000	Link
CVE-2023-26469	0.953540000	0.994220000	Link
CVE-2023-26360	0.964630000	0.996240000	Link
CVE-2023-26035	0.967750000	0.997140000	Link
CVE-2023-25717	0.950620000	0.993680000	Link
CVE-2023-25194	0.964550000	0.996210000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963230000	0.995900000	Link
CVE-2023-24489	0.972860000	0.998930000	Link
CVE-2023-23752	0.949000000	0.993440000	Link
CVE-2023-23333	0.960430000	0.995320000	Link
CVE-2023-22527	0.970410000	0.998030000	Link
CVE-2023-22518	0.959950000	0.995270000	Link
CVE-2023-22515	0.973650000	0.999250000	Link
CVE-2023-21839	0.941470000	0.992420000	Link
CVE-2023-21554	0.952650000	0.994080000	Link
CVE-2023-20887	0.970950000	0.998260000	Link
CVE-2023-1698	0.917150000	0.989930000	Link
CVE-2023-1671	0.962220000	0.995690000	Link
CVE-2023-0669	0.971830000	0.998530000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 11 Oct 2024

[NEU] [hoch] Red Hat Enterprise Linux (Advanced Cluster Management): Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder einen nicht spezifizierten Angriff durchzuführen.

- Link

—

Fri, 11 Oct 2024

[NEU] [kritisch] PaloAlto Networks Expedition: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in PaloAlto Networks Expedition ausnutzen, um beliebigen Code mit administrativen Rechten auszuführen, Daten zu manipulieren, einen Cross-Site-Scripting-Angriff durchzuführen und vertrauliche Informationen preiszugeben.

- Link

—

Fri, 11 Oct 2024

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

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Red Hat-Produkten ausnutzen, um Dateien zu manipulieren, beliebigen Code auszuführen und einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Fri, 11 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, 11 Oct 2024

[UPDATE] [hoch] Mozilla Firefox, Firefox ESR und Thunderbird: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Fri, 11 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

—

Fri, 11 Oct 2024

[UPDATE] [hoch] Oracle Communications: Mehrere Schwachstellen

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

- Link

—

Fri, 11 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

—

Fri, 11 Oct 2024

[UPDATE] [kritisch] Microsoft Windows: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in mehreren Versionen von Microsoft Windows und Microsoft Windows Server ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand zu erzeugen, Sicherheitsmaßnahmen zu umgehen und Plattform- und Service-Spoofing durchzuführen.

- Link

—

Fri, 11 Oct 2024

[UPDATE] [kritisch] PHP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um beliebigen Programmcode auszuführen, Informationen preiszugeben und andere nicht spezifizierte Angriffe durchzuführen.

- Link

—

Fri, 11 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, 11 Oct 2024

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

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

- Link

—

Fri, 11 Oct 2024

[UPDATE] [hoch] Ivanti Endpoint Manager Mobile: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein lokaler Angreifer kann eine Schwachstelle in Ivanti Endpoint Manager Mobile ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Fri, 11 Oct 2024

[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen und einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Fri, 11 Oct 2024

[UPDATE] [hoch] Juniper JUNOS: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Juniper JUNOS ausnutzen, um Denial-of-Service-Zustände herbeizuführen, Informationen preiszugeben, Code auszuführen, Privilegien zu erweitern und Sicherheitsmechanismen zu umgehen.

- Link

—

Thu, 10 Oct 2024

[UPDATE] [hoch] Grub2: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein Angreifer kann mehrere Schwachstellen in Oracle Linux ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Thu, 10 Oct 2024

[UPDATE] [hoch] vim: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und Dateien zu manipulieren.

- Link

—

Thu, 10 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, 10 Oct 2024

[UPDATE] [hoch] Linux “Shim”: Schwachstelle ermöglicht Übernahme der Kontrolle

Ein anonymer Angreifer aus dem angrenzenden Netzwerk kann eine Schwachstelle in der “Shim” Komponente von Linux-Systemen ausnutzen, um die Kontrolle über ein betroffenes System zu übernehmen.

- Link

—

Thu, 10 Oct 2024

[UPDATE] [hoch] util-linux: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein lokaler Angreifer kann eine Schwachstelle in util-linux ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
10/11/2024	[Mozilla Thunderbird < 128.3.1]	critical
10/11/2024	[Mozilla Thunderbird < 131.0.1]	critical
10/11/2024	[Mozilla Thunderbird < 115.16.0]	critical
10/11/2024	[Mozilla Thunderbird < 128.3.1]	critical
10/11/2024	[Mozilla Thunderbird < 131.0.1]	critical
10/11/2024	[Mozilla Thunderbird < 115.16.0]	critical
10/11/2024	[FreeBSD : firefox – use-after-free code execution (2fb13238-872d-11ef-bd1e-b42e991fc52e)]	critical
10/11/2024	[GitLab 12.5 < 17.2.9 / 17.3 < 17.3.5 / 17.4 < 17.4.2 (CVE-2024-9164)]	critical
10/11/2024	[Ivanti Policy Secure 22.x < 22.7R1.1 RCE]	critical
10/11/2024	[Ivanti Connect Secure 9.1Rx < 9.1R18.9 / 22.x < 22.7R2.1 RCE]	critical
10/11/2024	[Oracle Linux 8 : firefox (ELSA-2024-7977)]	critical
10/11/2024	[SUSE SLES12 Security Update : xen (SUSE-SU-2024:3586-1)]	high
10/11/2024	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2024:3587-1)]	high
10/11/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : libreoffice (SUSE-SU-2024:3577-1)]	high

Datum	Schwachstelle	Bewertung
10/11/2024	[Security Update for Microsoft Visual Studio Code (October 2024)]	high
10/11/2024	[Adobe Substance 3D Sampler 3.0.4 Multiple Vulnerabilities (apsb24-81)]	high
10/11/2024	[Siemens JT2Go < 2406.0003 Buffer Overflow (SSA-626178)]	high
10/11/2024	[Ivanti Endpoint Manager Mobile < 12.0.0.5, 12.1.x < 12.1.0.4 Improper Authorization (CVE-2024-7612)]	high
10/11/2024	[FreeBSD : vscode – Visual Studio Code for Linux Remote Code Execution Vulnerability (64e299b6-d12b-4a7a-a94f-ab133703925a)]	high
10/11/2024	[GitLab 11.6 < 17.2.9 / 17.3 < 17.3.5 / 17.4 < 17.4.2 (CVE-2024-8970)]	high
10/11/2024	[Ubuntu 22.04 LTS : Linux kernel vulnerabilities (USN-7020-4)]	high
10/11/2024	[Autodesk Navisworks Manage 25.0.x < 25.0.999.0 (2025.3) Multiple Vulnerabilities (adsk-sa-2024-0015)]	high
10/11/2024	[Autodesk Navisworks Simulate 25.0.x < 25.0.999.0 (2025.3) Multiple Vulnerabilities (adsk-sa-2024-0015)]	high
10/11/2024	[Autodesk Navisworks Freedom 25.0.x < 25.0.999.0 (2025.3) Multiple Vulnerabilities (adsk-sa-2024-0015)]	high
10/11/2024	[Security Updates for Microsoft Excel Products C2R (October 2024)]	high
10/11/2024	[Security Updates for Microsoft Office Products C2R (October 2024)]	high
10/11/2024	[Security Updates for Microsoft Visio Products C2R (October 2024)]	high
10/11/2024	[Progress Telerik Reporting <= 2024 Q3 (18.2.24.806) Multiple Vulnerabilities]	high
10/11/2024	[Apache Subversion < 1.14.4]	high
10/11/2024	[Security Updates for Microsoft Visual Studio Products (October 2024)]	high

Datum	Schwachstelle	Bewertung
10/11/2024	[Security Update for Microsoft .NET Core SDK (CVE-2024-38229) (October 2024)]	high
10/11/2024	[Security Update for Microsoft .NET Core SDK (October 2024)]	high
10/11/2024	[Progress Telerik UI for WinForms < 2024.3.924 Command Injection]	high
10/11/2024	[Security Updates for Microsoft .NET Framework (October 2024)]	high
10/11/2024	[CBL Mariner 2.0 Security Update: unbound (CVE-2024-33655)]	high
10/11/2024	[CBL Mariner 2.0 Security Update: nvidia-container-toolkit (CVE-2024-0132)]	high
10/11/2024	[AlmaLinux 9 : .NET 8.0 (ALSA-2024:7869)]	high
10/11/2024	[AlmaLinux 9 : .NET 6.0 (ALSA-2024:7867)]	high
10/11/2024	[HP Hotkey Support < 8.10.42.190 Privilege Escalation]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“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

—

” “Fri, 11 Oct 2024

Openfire 4.8.0 Code Injection

Openfire version 4.8.0 suffers from authentication bypass and code injection vulnerabilities.

- Link

—

” “Fri, 11 Oct 2024

MagnusBilling 6.x Code Injection

MagnusBilling version 6.x suffers from a PHP code injection vulnerability.

- Link

—

” “Fri, 11 Oct 2024

Kafka UI 0.7.1 Code Injection

Kafka UI version 0.7.1 suffers from a remote code injection vulnerability.

- Link

—

” “Fri, 11 Oct 2024

GL.iNet 4.4.3 Code Injection

GL.iNet version 4.4.3 suffers from authentication bypass and code injection vulnerabilities.

- Link

—

” “Fri, 11 Oct 2024

Gibbon School Platform 26.0.00 Code Injection

Gibbon School Platform version 26.0.00 suffers from a PHP code injection vulnerability.

- Link

—

” “Fri, 11 Oct 2024

Craft CMS 4.4.14 Code Injection

Craft CMS version 4.4.14 suffers from a PHP code injection vulnerability.

- Link

—

” “Fri, 11 Oct 2024

Chamilo 1.11.18 Code Injection

Chamilo version 1.11.18 suffers from a PHP code injection vulnerability.

- Link

—

” “Fri, 11 Oct 2024

Artica Proxy 4.40 Code Injection

Artica Proxy version 4.40 suffers from a code injection vulnerability that provides a reverse shell.

- Link

—

” “Thu, 10 Oct 2024

ABB Cylon Aspect 3.08.01 persistenceManagerAjax.php Directory Traversal

ABB Cylon Aspect version 3.08.01 has a directory traversal vulnerability that can be exploited by an unauthenticated attacker to list the contents of arbitrary directories without reading file contents, leading to information disclosure of directory structures and filenames. This may expose sensitive system details, aiding in further attacks. The issue lies in the listFiles() function of the persistenceManagerAjax.php script, which calls PHP’s readdir() function without proper input validation of the directory POST parameter.

- Link

—

” “Thu, 10 Oct 2024

Palo Alto Networks GlobalProtect Local Privilege Escalation

Palo Alto Networks GlobalProtect versions 5.1.x, 5.2.x, 6.0.x, 6.1.x, 6.3.x and versions less than 6.2.5 suffer from a local privilege escalation vulnerability.

- Link

—

” “Thu, 10 Oct 2024

Android GKI Kernels Use-After-Free

Android GKI kernels contain broken non-upstream Speculative Page Faults MM code that can lead to use-after-free conditions.

- Link

—

” “Wed, 09 Oct 2024

dav1d Integer Overflow / Out-Of-Bounds Write

There is an integer overflow in dav1d when decoding an AV1 video with large width/height. The integer overflow may result in an out-of-bounds write.

- Link

—

” “Tue, 08 Oct 2024

ABB Cylon Aspect 3.08.01 calendarFileDelete.php Arbitrary File Deletion

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

- Link

—

” “Tue, 08 Oct 2024

PHP-Nuke Top Module SQL Injection

The Top module for PHP-Nuke versions 6.x and below 7.6 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 07 Oct 2024

Grav CMS 1.7.44 Server-Side Template Injection

GenGravSSTIExploit is a proof of concept Python script that exploits an authenticated server-side template injection (SSTI) vulnerability in Grav CMS versions 1.7.44 and below. This vulnerability allows a user with editor permissions to execute OS commands on a remote server.

- Link

—

” “Mon, 07 Oct 2024

Ruby-SAML / GitLab Authentication Bypass

This script exploits the issue noted in CVE-2024-45409 that allows an unauthenticated attacker with access to any signed SAML document issued by the IDP to forge a SAML Response/Assertion and gain access as any user on GitLab. Ruby-SAML versions below or equal to 12.2 and versions 1.13.0 through

1.16.0 do not properly verify the signature of the SAML Response.
- Link

—

” “Mon, 07 Oct 2024

iTunes For Windows 12.13.2.3 Local Privilege Escalation

This is a thorough write up of how to exploit a local privilege escalation vulnerability in iTunes for Windows version 12.13.2.3. Apple fixed this in version 12.13.3.
- Link

—

” “Mon, 07 Oct 2024

ABB Cylon Aspect 3.08.00 syslogSwitch.php Remote Code Execution

ABB Cylon Aspect versions 3.08.00 and below suffer from an authenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the SYSLOG HTTP POST parameter called by the syslogSwitch.php script.
- Link

—

” “Mon, 07 Oct 2024

ABB Cylon Aspect 3.08.01 caldavUtil.php Remote Code Execution

ABB Cylon Aspect versions 3.08.01 and below suffer from an unauthenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the Footer HTTP POST parameter called by the caldavUtil.php script.
- Link

—

” “Mon, 07 Oct 2024

ABB Cylon Aspect 3.08.00 setTimeServer.php Remote Code Execution

ABB Cylon Aspect versions 3.08.00 and below suffer from an authenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the timeserver HTTP POST parameter called by the setTimeServer.php script.
- Link

—

”

4.2 0-Days der letzten 5 Tage

“Fri, 11 Oct 2024

ZDI-24-1381: Trimble SketchUp Viewer SKP File Parsing Memory Corruption Remote Code Execution Vulnerability
- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1380: Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1379: Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1378: Trimble SketchUp Viewer SKP File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1377: Trimble SketchUp Viewer SKP File Parsing Uninitialized Variable Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1376: Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1375: Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1374: IrfanView SID File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1373: IrfanView SID File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1372: IrfanView SID File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1371: IrfanView SID File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1370: IrfanView SID File Parsing Uninitialized Pointer Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1369: Zimbra GraphQL Cross-Site Request Forgery Information Disclosure Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1368: Tungsten Automation Power PDF JP2 File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1367: Tungsten Automation Power PDF JP2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1366: Tungsten Automation Power PDF PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1365: Tungsten Automation Power PDF JPF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1364: Tungsten Automation Power PDF JP2 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1363: Tungsten Automation Power PDF JP2 File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1362: Tungsten Automation Power PDF PDF File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1361: Tungsten Automation Power PDF AcroForm Annotation Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1360: Tungsten Automation Power PDF PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1359: Tungsten Automation Power PDF PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1358: Tungsten Automation Power PDF OXPS File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1357: Tungsten Automation Power PDF PNG File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1356: Tungsten Automation Power PDF GIF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1355: Tungsten Automation Power PDF PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1354: Tungsten Automation Power PDF JPG File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1353: Tungsten Automation Power PDF PDF File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1352: Tungsten Automation Power PDF PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1351: Tungsten Automation Power PDF PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1350: Tungsten Automation Power PDF PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1349: Tungsten Automation Power PDF PDF File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1348: Tungsten Automation Power PDF PNG File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1347: Tungsten Automation Power PDF TIF File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1346: Tungsten Automation Power PDF PDF File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1345: Tungsten Automation Power PDF TGA File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1344: Tungsten Automation Power PDF PSD File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1343: Tungsten Automation Power PDF BMP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1342: Tungsten Automation Power PDF PSD File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1341: Tungsten Automation Power PDF PDF File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1340: Tungsten Automation Power PDF PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1339: Tungsten Automation Power PDF XPS File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1338: Tungsten Automation Power PDF PDF File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1337: Tungsten Automation Power PDF XPS File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1336: Wacom Center WTabletServicePro Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1335: SonicWALL Connect Tunnel Link Following Denial-of-Service Vulnerability

- Link

—

” “Fri, 11 Oct 2024

ZDI-24-1334: SonicWALL Connect Tunnel Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Wed, 09 Oct 2024

ZDI-24-1333: NVIDIA Onyx Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1332: Adobe Dimension SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1331: Adobe Substance 3D Stager SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1330: Microsoft Windows win32kfull Use-After-Free Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1329: Axis Communications Autodesk Plugin AxisAddin axisapphelpfiles Remote Code Execution Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1328: Axis Communications Autodesk Plugin AzureBlobRestAPI axiscontentfiles Remote Code Execution Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1327: Ivanti Avalanche Faces ResourceManager Information Disclosure Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1326: Ivanti Avalanche SecureFilter allowPassThrough Authentication Bypass Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1325: Ivanti Avalanche SecureFilter Content-Type Authentication Bypass Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1324: Ivanti Avalanche validateAMCWSConnection Server-Side Request Forgery Information Disclosure Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1323: Centreon updateContactContactGroup SQL Injection Privilege Escalation Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1322: Centreon updateAccessGroupLinks SQL Injection Privilege Escalation Vulnerability

- Link

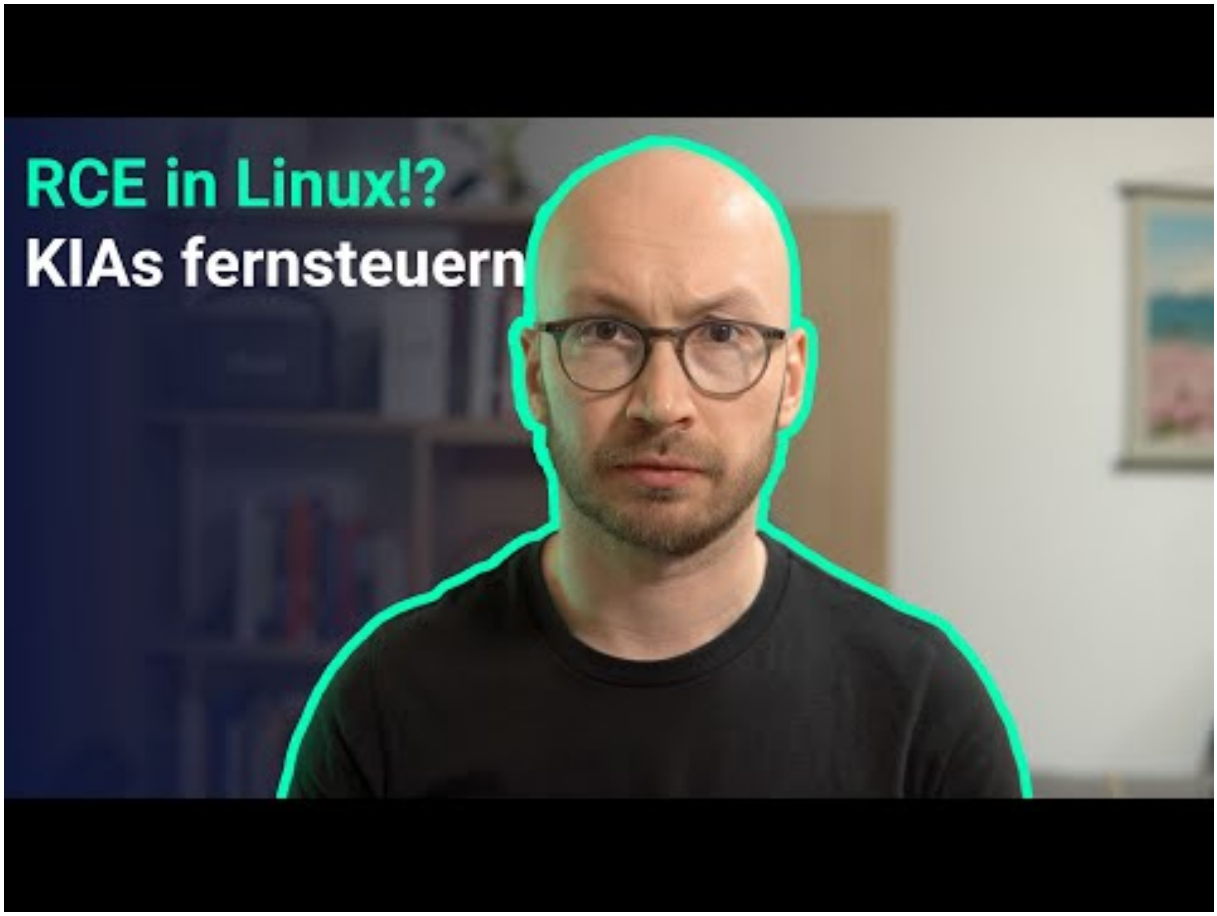
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Ein Grund mehr, Drucker zu hassen. Und Autos.



Zum Youtube Video

6 Cyberangriffe: (Okt)

Datum	Opfer	Land	Information
2024-10-10	Guajará-Mirim	[BRA]	Link
2024-10-10	Agence pour la Modernisation Administrative (AMA) du Portugal	[PRT]	Link
2024-10-08	Elbe-Heide	[DEU]	Link
2024-10-08	Nevada Joint Union High School District (NJUHSD)	[USA]	Link
2024-10-07	Vermilion Parish School System	[USA]	Link
2024-10-07	Axis Health System	[USA]	Link
2024-10-05	Casio Computer Co.	[JPN]	Link
2024-10-04	Groupe Hospi Grand Ouest	[FRA]	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
2024-10-01	Oyonnax	[FRA]	Link
2024-10-01	C.R. Laurence (CRL)	[USA]	Link

7 Ransomware-Erpressungen: (Okt)

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-10-11	[Rumpke Consolidated Companies]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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	[practicesuite.us]	ransomhub	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.it]	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
2024-10-04	[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
2024-10-03	[Golden Age Nursing Home]	rhysida	Link
2024-10-02	[domainindustries.com]	ransomhub	Link
2024-10-02	[ironmetals.com]	ransomhub	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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.