
Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250122



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	18
5 Die Hacks der Woche	22
5.0.1 Gehackt via Nachbar... oder die Palo Alto.	22
6 Cyberangriffe: (Jan)	23
7 Ransomware-Erpressungen: (Jan)	23
8 Quellen	34
8.1 Quellenverzeichnis	34
9 Impressum	35

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

7-Zip: Lücke erlaubt Umgehung von Mark-of-the-Web

In 7-Zip ermöglicht eine Sicherheitslücke, den Mark-of-the-Web-Schutzmechanismus auszuhebeln und so Code auszuführen. Ein Update ist verfügbar.

- [Link](#)

—

Webbrowser: Brave-Sicherheitsleck sorgt für falsch angezeigte Download-Quelle

Im Webbrowser Brave können Angreifer eine Sicherheitslücke missbrauchen, die zur falschen Anzeige einer Download-Quelle führt.

- [Link](#)

—

Sicherheitspatch: Unbefugte Zugriffe auf bestimmte Switches von Moxa möglich

Angreifer können bei Moxa-Switches der EDS-508A-Serie die Authentifizierung umgehen. Die Sicherheitslücke gilt als kritisch.

- [Link](#)

—

Nvidia: Datenabfluss durch Sicherheitsleck in Grafiktreiber möglich

Nvidia hat Sicherheitslücken in seinen Grafikkartentreibern entdeckt. Angreifer können dadurch Informationen abgreifen. Updates stehen bereit.

- [Link](#)

—

WordPress-Plug-in W3 Total Cache: Potenziell 1 Millionen Websites attackierbar

Stimmen die Voraussetzungen, können Angreifer Websites mit dem WordPress-Plug-in W3 Total Cache ins Visier nehmen. Ein Sicherheitspatch ist verfügbar.

- [Link](#)

—

Es kann Schadcode auf HPE Aruba Networking AOS Controllers und Gateways gelangen

Netzwerktechnik von HPE Aruba ist verwundbar. Aktuelle Updates schließen insgesamt zwei Sicherheitslücken.

- [Link](#)

—

Updates gegen Lecks in Ivanti Application Control Engine, Avalanche und EPM

Ivanti hat Sicherheitsupdates für Application Control Engine, Avalanche und EPM veröffentlicht. Sie bessern teils kritische Lecks aus.

- [Link](#)

Kopierdienst rsync mit kritischer Lücke

Sicherheitsforscher entdeckten Lücken in der Open-Source-Software rsync, mit der man sehr effizient Dateien synchronisieren oder auch nur kopieren kann.

- [Link](#)

Jetzt patchen! Attacken auf Netzwerkgeräte von Fortinet beobachtet

Der Anbieter von IT-Securitylösungen Fortinet hat zahlreiche Sicherheitsupdates für seine Produkte veröffentlicht. Eine Lücke wird bereits ausgenutzt.

- [Link](#)

CMS: Typo3-Entwickler dichten zehn Sicherheitslücken ab

Das Content-Management-System Typo3 schließt mit aktualisierten Paketen zehn Sicherheitslücken.

- [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	0.933570000	0.993070000	Link
CVE-2023-6895	0.926080000	0.992440000	Link
CVE-2023-6553	0.959610000	0.996240000	Link
CVE-2023-6019	0.942220000	0.993960000	Link
CVE-2023-6018	0.926470000	0.992470000	Link
CVE-2023-52251	0.953810000	0.995340000	Link
CVE-2023-4966	0.952900000	0.995240000	Link
CVE-2023-49103	0.952840000	0.995220000	Link
CVE-2023-48795	0.954830000	0.995510000	Link
CVE-2023-48788	0.967910000	0.997970000	Link
CVE-2023-47246	0.959320000	0.996220000	Link
CVE-2023-46805	0.966650000	0.997670000	Link
CVE-2023-46747	0.972880000	0.999340000	Link
CVE-2023-46604	0.970170000	0.998560000	Link
CVE-2023-4542	0.929810000	0.992770000	Link
CVE-2023-43208	0.974800000	0.999850000	Link
CVE-2023-43177	0.966220000	0.997570000	Link
CVE-2023-42793	0.974850000	0.999870000	Link
CVE-2023-4220	0.954100000	0.995390000	Link
CVE-2023-39143	0.920920000	0.992050000	Link
CVE-2023-38035	0.972090000	0.999150000	Link
CVE-2023-35813	0.921490000	0.992120000	Link
CVE-2023-3519	0.964000000	0.997090000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-35082	0.960390000	0.996370000	Link
CVE-2023-35078	0.969340000	0.998330000	Link
CVE-2023-34993	0.968280000	0.998050000	Link
CVE-2023-34634	0.908890000	0.991170000	Link
CVE-2023-34362	0.971720000	0.999020000	Link
CVE-2023-34105	0.948800000	0.994690000	Link
CVE-2023-34039	0.958830000	0.996160000	Link
CVE-2023-3368	0.937700000	0.993510000	Link
CVE-2023-33246	0.973200000	0.999470000	Link
CVE-2023-32315	0.970190000	0.998580000	Link
CVE-2023-32235	0.929990000	0.992790000	Link
CVE-2023-30625	0.948340000	0.994630000	Link
CVE-2023-30013	0.968230000	0.998040000	Link
CVE-2023-29298	0.971810000	0.999050000	Link
CVE-2023-28432	0.931990000	0.992970000	Link
CVE-2023-28343	0.966300000	0.997580000	Link
CVE-2023-28121	0.910260000	0.991260000	Link
CVE-2023-27524	0.972590000	0.999250000	Link
CVE-2023-27372	0.973390000	0.999520000	Link
CVE-2023-27350	0.968700000	0.998180000	Link
CVE-2023-26469	0.957270000	0.995870000	Link
CVE-2023-26035	0.969170000	0.998300000	Link
CVE-2023-25717	0.953520000	0.995310000	Link
CVE-2023-25194	0.960710000	0.996430000	Link
CVE-2023-2479	0.966080000	0.997530000	Link
CVE-2023-24489	0.972390000	0.999210000	Link
CVE-2023-23752	0.937230000	0.993470000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23333	0.962780000	0.996830000	Link
CVE-2023-22527	0.972290000	0.999180000	Link
CVE-2023-22518	0.969410000	0.998340000	Link
CVE-2023-22515	0.969730000	0.998450000	Link
CVE-2023-20887	0.972060000	0.999130000	Link
CVE-2023-1671	0.957150000	0.995850000	Link
CVE-2023-0669	0.971020000	0.998850000	Link
CVE-2023-0297	0.948640000	0.994660000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 21 Jan 2025

[UPDATE] [hoch] Google Chrome und Microsoft Edge: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Tue, 21 Jan 2025

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um einen Denial of Service Zustand herbeizuführen oderum einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Tue, 21 Jan 2025

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

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um Informationen offenzulegen, einen Denial of Service zu verursachen, Code zur Ausführung zu bringen und weitere, nicht spezifizierte Auswirkungen herbeizuführen.

- [Link](#)

—

Tue, 21 Jan 2025

[UPDATE] [hoch] Red Hat Enterprise Linux und OpenShift (go-git): Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux in der Grafana Komponente ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen preiszugeben und einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Mon, 20 Jan 2025

[NEU] [hoch] Moxa Switch: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Moxa Switch ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Mon, 20 Jan 2025

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Mon, 20 Jan 2025

[UPDATE] [hoch] BusyBox: Mehrere Schwachstellen

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in BusyBox ausnutzen, um einen Denial of Service Angriff durchzuführen, Informationen offenzulegen oder beliebigen Code auszuführen.

- [Link](#)

—

Mon, 20 Jan 2025

[UPDATE] [hoch] Node.js: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um einen Denial of Service Angriff durchzuführen oder Code zur Ausführung zu bringen.

- [Link](#)

—

Mon, 20 Jan 2025

[UPDATE] [hoch] BusyBox: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in BusyBox ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Mon, 20 Jan 2025

[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](#)

—

Mon, 20 Jan 2025

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

Ein entfernter, anonym 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](#)

—

Mon, 20 Jan 2025

[UPDATE] [hoch] bluez: Schwachstelle ermöglicht Codeausführung

Ein Angreifer aus einem angrenzenden Netzwerk kann eine Schwachstelle in bluez ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Mon, 20 Jan 2025

[UPDATE] [hoch] MediaWiki: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in MediaWiki ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Cross-Site-Scripting-Angriff durchzuführen oder Dateien zu manipulieren.

- [Link](#)

—

Mon, 20 Jan 2025

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Denial of Service

Ein Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um einen Denial of Service Angriff durchzuführen oder nicht näher beschriebene Auswirkungen zu erzielen.

- [Link](#)

—

Mon, 20 Jan 2025

[UPDATE] [hoch] Python “virtualenv”: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonym Angreifer kann eine Schwachstelle im Python “virtualenv” Paket ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Mon, 20 Jan 2025

[UPDATE] [hoch] Apache Tomcat: Mehrere Schwachstellen

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Apache Tomcat ausnutzen, um beliebigen Programmcode auszuführen und einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Mon, 20 Jan 2025

[UPDATE] [hoch] Apache Tomcat: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymmer Angreifer kann eine Schwachstelle in Apache Tomcat ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Mon, 20 Jan 2025

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

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Firefox ESR und Thunderbird ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, vertrauliche Informationen preiszugeben, Sicherheitsmaßnahmen zu umgehen oder Spoofing-Angriffe durchzuführen.

- [Link](#)

—

Mon, 20 Jan 2025

[UPDATE] [hoch] Microsoft Developer Tools: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Microsoft Visual Studio 2017, Microsoft .NET Framework, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022, Microsoft Visual Studio 2019, Microsoft Visual Studio 2022 und Microsoft Windows ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen und vertrauliche Informationen preiszugeben.

- [Link](#)

—

Mon, 20 Jan 2025

[UPDATE] [kritisch] Microsoft Windows: Mehrere Schwachstellen

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

- [Link](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
1/21/2025	[EulerOS 2.0 SP8 : httpd (EulerOS-SA-2025-1122)]	critical
1/21/2025	[EulerOS 2.0 SP8 : kernel (EulerOS-SA-2025-1123)]	critical
1/21/2025	[EulerOS 2.0 SP8 : openssl (EulerOS-SA-2025-1126)]	critical
1/21/2025	[EulerOS 2.0 SP8 : wget (EulerOS-SA-2025-1130)]	critical
1/21/2025	[EulerOS 2.0 SP8 : docker-engine (EulerOS-SA-2025-1119)]	critical
1/21/2025	[EulerOS 2.0 SP8 : git (EulerOS-SA-2025-1121)]	critical
1/21/2025	[EulerOS 2.0 SP8 : krb5 (EulerOS-SA-2025-1124)]	critical
1/21/2025	[EulerOS 2.0 SP8 : ruby (EulerOS-SA-2025-1129)]	critical
1/21/2025	[EulerOS 2.0 SP8 : freerdp (EulerOS-SA-2025-1120)]	critical
1/21/2025	[Debian dla-4027 : sympa - security update]	critical
1/21/2025	[RHEL 8 / 9 : Red Hat JBoss Web Server 6.0.5 (RHSA-2025:0342)]	critical
1/21/2025	[Debian dsa-5847 : snapclient - security update]	critical
1/21/2025	[RHEL 8 : grafana (RHSA-2025:0401)]	critical
1/21/2025	[Fedora 41 : rsync (2025-3ec637e6e9)]	critical
1/21/2025	[Amazon Corretto Java 17.x < 17.0.14.7.1 Vulnerability]	critical
1/20/2025	[Debian dla-4024 : libpoco-dev - security update]	critical
1/21/2025	[Node.js 18.x < 18.20.6 / 20.x < 20.18.2 / 22.x < 22.13.1 / 23.x < 23.6.1 Multiple Vulnerabilities (Tuesday, January 21, 2025 Security Releases).]	high
1/21/2025	[EulerOS 2.0 SP8 : cups-filters (EulerOS-SA-2025-1118)]	high
1/21/2025	[EulerOS 2.0 SP8 : libgsf (EulerOS-SA-2025-1125)]	high
1/21/2025	[EulerOS 2.0 SP8 : perl-App-cpanminus (EulerOS-SA-2025-1127)]	high
1/21/2025	[RHEL 9 : .NET 8.0 (RHSA-2025:0532)]	high

Datum	Schwachstelle	Bewertung
1/21/2025	[RHEL 9 : iperf3 (RHSA-2025:0505)]	high
1/21/2025	[RHEL 8 : iperf3 (RHSA-2025:0548)]	high
1/21/2025	[RHEL 9 : iperf3 (RHSA-2025:0440)]	high
1/21/2025	[Debian dla-4016 : ucf - security update]	high
1/21/2025	[SUSE SLES15 Security Update : kernel (Live Patch 33 for SLE 15 SP4) (SUSE-SU-2025:0184-1)]	high
1/21/2025	[SUSE SLES15 Security Update : kernel (Live Patch 1 for SLE 15 SP6) (SUSE-SU-2025:0187-1)]	high
1/21/2025	[SUSE SLES15 Security Update : kernel (Live Patch 32 for SLE 15 SP4) (SUSE-SU-2025:0185-1)]	high
1/21/2025	[SUSE SLES15 Security Update : pam_u2f (SUSE-SU-2025:0192-1)]	high
1/21/2025	[SUSE SLES15 Security Update : kernel (Live Patch 2 for SLE 15 SP6) (SUSE-SU-2025:0188-1)]	high
1/21/2025	[SUSE SLES15 Security Update : kernel (Live Patch 48 for SLE 15 SP3) (SUSE-SU-2025:0180-1)]	high
1/21/2025	[SUSE SLES15 Security Update : kernel (Live Patch 17 for SLE 15 SP5) (SUSE-SU-2025:0181-1)]	high
1/21/2025	[RHEL 8 : iperf3 (RHSA-2025:0403)]	high
1/21/2025	[RHEL 9 : redis (RHSA-2025:0400)]	high
1/21/2025	[RHEL 9 : redis (RHSA-2025:0399)]	high
1/21/2025	[RHEL 9 : redis (RHSA-2025:0398)]	high
1/21/2025	[RHEL 7 : iperf3 (RHSA-2025:0402)]	high
1/21/2025	[RHEL 8 : iperf3 (RHSA-2025:0404)]	high
1/21/2025	[openSUSE 15 Security Update : chromium (openSUSE-SU-2025:0018-1)]	high
1/21/2025	[Fedora 40 : dotnet9.0 (2024-b13025f236)]	high
1/21/2025	[Ubuntu 24.04 LTS / 24.10 : Python vulnerability (USN-7219-1)]	high

Datum	Schwachstelle	Bewertung
1/21/2025	[Amazon Corretto Java 11.x < 11.0.26.4.1 Vulnerability]	high
1/20/2025	[Debian dla-4018 : libruby2.7 - security update]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Tue, 03 Dec 2024

Acronis Cyber Protect/Backup Remote Code Execution

The Acronis Cyber Protect appliance, in its default configuration, allows the anonymous registration of new protect/backup agents on new endpoints. This API endpoint also generates bearer tokens which the agent then uses to authenticate to the appliance. As the management web console is running on the same port as the API for the agents, this bearer token is also valid for any actions on the web console. This allows an attacker with network access to the appliance to start the registration of a new agent, retrieve a bearer token that provides admin access to the available functions in the web console. The web console contains multiple possibilities to execute arbitrary commands on both the agents (e.g., via PreCommands for a backup) and also the appliance (e.g., via a Validation job on the agent of the appliance). These options can easily be set with the provided bearer token, which leads to a complete compromise of all agents and the appliance itself.

- [Link](#)

—

” “Tue, 03 Dec 2024

Fortinet FortiManager Unauthenticated Remote Code Execution

This Metasploit module exploits a missing authentication vulnerability affecting FortiManager and FortiManager Cloud devices to achieve unauthenticated RCE with root privileges. The vulnerable FortiManager versions are 7.6.0, 7.4.0 through 7.4.4, 7.2.0 through 7.2.7, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, and 6.2.0 through 6.2.12. The vulnerable FortiManager Cloud versions are 7.4.1 through 7.4.4, 7.2.1 through 7.2.7, 7.0.1 through 7.0.12, and 6.4 (all versions).

- [Link](#)

—

” “Tue, 03 Dec 2024

Asterisk AMI Originate Authenticated Remote Code Execution

On Asterisk, prior to versions 18.24.2, 20.9.2, and 21.4.2 and certified-asterisk versions 18.9-cert11 and 20.7-cert2, an AMI user with write=originate may change all configuration files in the /etc/asterisk/

directory. Writing a new extension can be created which performs a system command to achieve RCE as the asterisk service user (typically asterisk). Default parking lot in FreePBX is called "Default lot" on the website interface, however its actually parkedcalls. Tested against Asterisk 19.8.0 and 18.16.0 on Freepbx SNG7-PBX16-64bit-2302-1.

- [Link](#)

—

" "Mon, 02 Dec 2024

Omada Identity Cross Site Scripting

Omada Identity versions prior to 15U1 and 14.14 hotfix #309 suffer from a persistent cross site scripting vulnerability.

- [Link](#)

—

" "Mon, 02 Dec 2024

Siemens Unlocked JTAG Interface / Buffer Overflow

Various Siemens products suffer from vulnerabilities. There is an unlocked JTAG Interface for Zynq-7000 on SM-2558 and a buffer overflow on the webserver of the SM-2558, CP-2016, and CP-2019 systems.

- [Link](#)

—

" "Mon, 02 Dec 2024

ABB Cylon Aspect 3.08.00 fileSystemUpdate.php File Upload / Denial Of Service

ABB Cylon Aspect version 3.08.00 suffers from a vulnerability in the fileSystemUpdate.php endpoint of the ABB BEMS controller due to improper handling of uploaded files. The endpoint lacks restrictions on file size and type, allowing attackers to upload excessively large or malicious files. This flaw could be exploited to cause denial of service (DoS) attacks, memory leaks, or buffer overflows, potentially leading to system crashes or further compromise.

- [Link](#)

—

" "Mon, 02 Dec 2024

ABB Cylon Aspect 3.08.01 mstpstatus.php Information Disclosure

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated information disclosure vulnerability. An unauthorized attacker can reference the affected page and disclose various BACnet MS/TP statistics running on the device.

- [Link](#)

—

" "Mon, 02 Dec 2024

ABB Cylon Aspect 3.08.01 diagLateThread.php Information Disclosure

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated information disclosure vulnerabi-

lity. An unauthorized attacker can reference the affected page and disclose various protocol thread information running on the device.

- [Link](#)

—

” “Mon, 02 Dec 2024

AppleAVD AV1_Syntax::Parse_Header Out-Of-Bounds Reads

AppleAVD has an issue where a large OBU size in AV1_Syntax::Parse_Header reading can lead to out-of-bounds reads.

- [Link](#)

—

” “Mon, 02 Dec 2024

AppleAVD AV1_Syntax::f Out-Of-Bounds Reads

AppleAVD has an issue in AV1_Syntax::f leading to out-of-bounds reads.

- [Link](#)

—

” “Mon, 02 Dec 2024

AppleAVD AV1_Syntax::Parse_Header Integer Underflow / Out-Of-Bounds Reads

AppleAVD has an integer underflow in AV1_Syntax::Parse_Header that can lead to out-of-bounds reads.

- [Link](#)

—

” “Mon, 02 Dec 2024

Simple Chat System 1.0 Cross Site Scripting

Simple Chat System version 1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 02 Dec 2024

Russian FSB Cross Site Scripting

The Russian FSB appears to suffer from a cross site scripting vulnerability. The researchers who discovered it have reported it multiple times to them.

- [Link](#)

—

” “Mon, 02 Dec 2024

Laravel 11.0 Cross Site Scripting

Laravel version 11.0 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 02 Dec 2024

Nvidia GeForce 11.0.1.163 Unquoted Service Path

Nvidia GeForce version 11.0.1.163 suffers from an unquoted service path vulnerability.

- [Link](#)

—

” “Mon, 02 Dec 2024

Intelligent Security System SecurOS Enterprise 11 Unquoted Service Path

Intelligent Security System SecurOS Enterprise version 11 suffers from an unquoted service path vulnerability.

- [Link](#)

—

” “Wed, 27 Nov 2024

ABB Cylon Aspect 3.08.01 vstatConfigurationDownload.php Configuration Download

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

- [Link](#)

—

” “Wed, 27 Nov 2024

Akuvox Smart Intercom/Doorphone ServicesHTTPAPI Improper Access Control

The Akuvox Smart Intercom/Doorphone suffers from an insecure service API access control. The vulnerability in ServicesHTTPAPI endpoint allows users with "User" privileges to modify API access settings and configurations. This improper access control permits privilege escalation, enabling unauthorized access to administrative functionalities. Exploitation of this issue could compromise system integrity and lead to unauthorized system modifications.

- [Link](#)

—

” “Fri, 22 Nov 2024

CUPS IPP Attributes LAN Remote Code Execution

This Metasploit module exploits vulnerabilities in OpenPrinting CUPS, which is running by default on most Linux distributions. The vulnerabilities allow an attacker on the LAN to advertise a malicious printer that triggers remote code execution when a victim sends a print job to the malicious printer. Successful exploitation requires user interaction, but no CUPS services need to be reachable via accessible ports. Code execution occurs in the context of the lp user. Affected versions are cups-browsed less than or equal to 2.0.1, libcupsfilters versions 2.1b1 and below, libppd versions 2.1b1 and below, and cups-filters versions 2.0.1 and below.

- [Link](#)

—

” “Fri, 22 Nov 2024

ProjectSend R1605 Unauthenticated Remote Code Execution

This Metasploit module exploits an improper authorization vulnerability in ProjectSend versions r1295 through r1605. The vulnerability allows an unauthenticated attacker to obtain remote code execution by enabling user registration, disabling the whitelist of allowed file extensions, and uploading a malicious PHP file to the server.

- [Link](#)

—

” “Fri, 22 Nov 2024

needrestart Local Privilege Escalation

Qualys discovered that needrestart suffers from multiple local privilege escalation vulnerabilities that allow for root access from an unprivileged user.

- [Link](#)

—

” “Fri, 22 Nov 2024

fronsetia 1.1 Cross Site Scripting

fronsetia version 1.1 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Fri, 22 Nov 2024

fronsetia 1.1 XML Injection

fronsetia version 1.1 suffers from an XML external entity injection vulnerability.

- [Link](#)

—

” “Fri, 22 Nov 2024

PowerVR psProcessHandleBase Reuse

PowerVR has an issue where PVRSRVAcquireProcessHandleBase() can cause psProcessHandleBase reuse when PIDs are reused.

- [Link](#)

—

” “Fri, 22 Nov 2024

Linux 6.6 Race Condition

A security-relevant race between mremap() and THP code has been discovered. Reaching the buggy code typically requires the ability to create unprivileged namespaces. The bug leads to installing physical address 0 as a page table, which is likely exploitable in several ways: For example, triggering the bug in multiple processes can probably lead to unintended page table sharing, which probably can lead to stale TLB entries pointing to freed pages.

- [Link](#)

—
”

4.2 0-Days der letzten 5 Tage

“Mon, 20 Jan 2025

ZDI-25-055: Sante PACS Server URL path Memory Corruption Denial-of-Service Vulnerability

- [Link](#)

—

” “Mon, 20 Jan 2025

ZDI-25-054: Sante PACS Server Web Portal DCM File Parsing Directory Traversal Arbitrary File Write Vulnerability

- [Link](#)

—

” “Mon, 20 Jan 2025

ZDI-25-053: Sante PACS Server DCM File Parsing Directory Traversal Arbitrary File Write Vulnerability

- [Link](#)

—

” “Mon, 20 Jan 2025

ZDI-25-052: Sante PACS Server DCM File Parsing Memory Corruption Denial-of-Service Vulnerability

- [Link](#)

—

” “Mon, 20 Jan 2025

ZDI-25-051: Sante PACS Server Web Portal DCM File Parsing Memory Corruption Denial-of-Service Vulnerability

- [Link](#)

—

” “Mon, 20 Jan 2025

ZDI-25-050: Sante PACS Server Web Portal DCM File Parsing Memory Corruption Denial-of-Service Vulnerability

- [Link](#)

—

” “Mon, 20 Jan 2025

ZDI-25-049: Sante PACS Server DCM File Parsing Memory Corruption Denial-of-Service Vulnerability

- [Link](#)

—
” “Mon, 20 Jan 2025

ZDI-25-048: Apple WebKit WebCore ContainerNode Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

—
” “Mon, 20 Jan 2025

ZDI-25-047: WinZip 7Z File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

—
” “Mon, 20 Jan 2025

ZDI-25-046: Adobe Photoshop node_modules Uncontrolled Search Path Element Local Privilege Escalation Vulnerability

- [Link](#)

—
” “Sun, 19 Jan 2025

ZDI-25-045: 7-Zip Mark-of-the-Web Bypass Vulnerability

- [Link](#)

—
” “Sun, 19 Jan 2025

ZDI-25-044: Ivanti Avalanche SecureFilter Authentication Bypass Vulnerability

- [Link](#)

—
” “Sun, 19 Jan 2025

ZDI-25-043: Ivanti Avalanche Faces ResourceManager Information Disclosure Vulnerability

- [Link](#)

—
” “Sun, 19 Jan 2025

ZDI-25-042: Ivanti Avalanche SecureFilter allowPassThrough Authentication Bypass Vulnerability

- [Link](#)

—
” “Sun, 19 Jan 2025

ZDI-25-041: Ivanti Endpoint Manager updateAssetInfo SQL Injection Remote Code Execution Vulnerability

- [Link](#)

—
” “Sun, 19 Jan 2025

ZDI-25-040: Ivanti Endpoint Manager DecodeBase64Object Deserialization of Untrusted Data

Remote Code Execution Vulnerability

- [Link](#)

—

” “Sun, 19 Jan 2025

ZDI-25-039: Ivanti Endpoint Manager AlertService Uninitialized Memory Information Disclosure Vulnerability

- [Link](#)

—

” “Sun, 19 Jan 2025

ZDI-25-038: Ivanti Endpoint Manager Improper Input Validation AlertService Denial-of-Service Vulnerability

- [Link](#)

—

” “Sun, 19 Jan 2025

ZDI-25-037: Ivanti Endpoint Manager AlertService Improper Input Validation Denial-of-Service Vulnerability

- [Link](#)

—

” “Sun, 19 Jan 2025

ZDI-25-036: Ivanti Endpoint Manager AlertService Improper Input Validation Denial-of-Service Vulnerability

- [Link](#)

—

” “Sun, 19 Jan 2025

ZDI-25-035: Ivanti Endpoint Manager AlertService Improper Input Validation Denial-of-Service Vulnerability

- [Link](#)

—

” “Sun, 19 Jan 2025

ZDI-25-034: Ivanti Endpoint Manager AlertService Type Confusion Information Disclosure Vulnerability

- [Link](#)

—

” “Sun, 19 Jan 2025

ZDI-25-033: Ivanti Endpoint Manager AlertService Improper Input Validation Denial-of-Service Vulnerability

- [Link](#)

—

” “Sun, 19 Jan 2025

ZDI-25-032: Ivanti Endpoint Manager HllDriver Improper Verification of Cryptographic Signature Remote Code Execution Vulnerability

- [Link](#)

—

” “Sun, 19 Jan 2025

ZDI-25-031: Ivanti Endpoint Manager MyResolveEventHandler Untrusted Search Path Remote Code Execution Vulnerability

- [Link](#)

—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Gehackt via Nachbar... oder die Palo Alto.



[Zum Youtube Video](#)

6 Cyberangriffe: (Jan)

Datum	Opfer	Land	Information
2025-01-17	Blacon High School	[GBR]	Link
2025-01-15	Schul-IT in Speyer	[DEU]	Link
2025-01-13	Aurora Public Schools	[USA]	Link
2025-01-13	D-Trust GmbH	[DEU]	Link
2025-01-13	CHU de Grenoble Alpes	[FRA]	Link
2025-01-12	Technische Universiteit Eindhoven (TU Eindhoven)	[NLD]	Link
2025-01-11	Bourne	[USA]	Link
2025-01-08	Office of Geodesy, Cartography and Cadastre of the Slovak Republic (UGKK)	[SVK]	Link
2025-01-08	Prefeitura de Sarapuí	[BRA]	Link
2025-01-08	Gateshead Council	[GBR]	Link
2025-01-08	University of Oklahoma	[USA]	Link
2025-01-07	Addison Northwest School District (ANWSD)	[USA]	Link
2025-01-07	New Brunswick Liquor Corporation	[CAN]	Link
2025-01-07	Laramie County Library System	[USA]	Link
2025-01-05	South Portland Public Schools	[USA]	Link
2025-01-05	Upper Canada District School Board (UCDSB)	[CAN]	Link
2025-01-04	Un hôtel à Großarl	[AUT]	Link
2025-01-03	La Police de Kingston	[CAN]	Link

7 Ransomware-Erpressungen: (Jan)

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-01-22	[JOMARSOFTCORP.COM]	clop	Link
2025-01-22	[www.americanstandard-us.com]	ransomhub	Link
2025-01-22	[Christian Community Aid]	spacebears	Link
2025-01-22	[SANTA MARIA LABORATORIO]	spacebears	Link
2025-01-22	[Jacobs & Thompson]	lynx	Link
2025-01-22	[Mintz Law Firm, LLC]	lynx	Link
2025-01-21	[Solaris-pharma.com]	everest	Link
2025-01-21	[semesco.com]	safepay	Link
2025-01-21	[brunetti.com]	safepay	Link
2025-01-21	[solge.es]	safepay	Link
2025-01-21	[precisionmechsd.com]	ransomhub	Link
2025-01-21	[whychoosebw.com]	ransomhub	Link
2025-01-21	[boardman-hamilton.com]	ransomhub	Link
2025-01-21	[miedemaproduce.com]	ransomhub	Link
2025-01-21	[RETAL Baltic Films]	incransom	Link
2025-01-21	[navy-mil-bd]	funksec	Link
2025-01-21	[ayswrewards.cow]	funksec	Link
2025-01-21	[icicibank.com]	apt73	Link
2025-01-21	[Moinho GloboAlimentos]	akira	Link
2025-01-21	[Inaya Clinique]	spacebears	Link
2025-01-21	[supremegroup.co.in]	ransomhub	Link
2025-01-21	[FAAB Invest Advisors Private Limited]	killsec	Link
2025-01-21	[Nimbus Facility Services]	killsec	Link
2025-01-21	[cu-barika.dz]	funksec	Link
2025-01-21	[thecitybank.com]	funksec	Link
2025-01-21	[insta.com.pk]	funksec	Link
2025-01-21	[Bethany Hospital]	spacebears	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-01-21	[Marukai]	lynx	Link
2025-01-20	[PetroVietnam Exploration Production Corporation]	hunters	Link
2025-01-20	[theurswickschool.co.uk]	kairos	Link
2025-01-20	[malindoair.com]	apt73	Link
2025-01-20	[Delta Fabrication and Machine, Inc]	medusa	Link
2025-01-20	[D & M Trim]	medusa	Link
2025-01-20	[Jacquet Weston Engineering]	sarcoma	Link
2025-01-20	[compass-underwriting-ltd]	sarcoma	Link
2025-01-20	[cana group corp]	sarcoma	Link
2025-01-20	[Rabwin]	qilin	Link
2025-01-20	[Zuk Group]	handala	Link
2025-01-20	[Clutch Industries]	lynx	Link
2025-01-20	[Sentinel Systems]	lynx	Link
2025-01-20	[Angotti & Reilly]	lynx	Link
2025-01-19	[TG3 Electronics]	rhysida	Link
2025-01-19	[Richardson]	qilin	Link
2025-01-19	[WELKER	World-Class Manufacturing]	qilin
2025-01-18	[MERCURYGATE.COM]	clop	Link
2025-01-18	[USE Federal Credit Union]	qilin	Link
2025-01-18	[Refreshment Services Pepsi]	qilin	Link
2025-01-18	[Marina Family Medical]	moneymessage	Link
2025-01-18	[MassDevelopment]	bianlian	Link
2025-01-18	[gonzalesusd.net]	safepay	Link
2025-01-18	[Kassin & Carrow]	lynx	Link
2025-01-17	[Gossett Motor Cars]	lynx	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-01-17	[nightingalehammerson.org]	kairos	Link
2025-01-17	[fol-23.fr]	apt73	Link
2025-01-17	[aquamanaesp.gov.co]	funksec	Link
2025-01-17	[Divimast]	akira	Link
2025-01-17	[VODOTEHNIKA D.D.]	akira	Link
2025-01-17	[Chain And Rope SuppliersLTD]	akira	Link
2025-01-17	[realtaxcanada.com]	kairos	Link
2025-01-17	[LYNXSPA]	morpheus	Link
2025-01-17	[Washington Gastroenterology (DHSWA.NET)]	incransom	Link
2025-01-17	[Kilgore College (kilgore.edu)]	incransom	Link
2025-01-17	[peponline.org]	incransom	Link
2025-01-17	[Taylor Regional Hospital (thcg.local)]	incransom	Link
2025-01-17	[Regina Coeli Convent]	incransom	Link
2025-01-09	[platinumcollision.com]	safepay	Link
2025-01-16	[Woodlake]	everest	Link
2025-01-16	[Volt Infrastructure]	everest	Link
2025-01-16	[The Hoff Brand SL]	everest	Link
2025-01-16	[Dona Formosa]	sarcoma	Link
2025-01-16	[JD Lighting]	sarcoma	Link
2025-01-16	[Farmacia Cofar]	killsec	Link
2025-01-16	[anupalanonline.com]	killsec	Link
2025-01-16	[Netform GmbH]	8base	Link
2025-01-16	[Delta Dental of Washington]	8base	Link
2025-01-16	[bsegroup.it]	ransomhub	Link
2025-01-16	[www.solariumrevestimentos.com.br]	ransomhub	Link
2025-01-16	[www.liteputer.com.tw]	ransomhub	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-01-16	[Access Capital Partners SA]	lynx	Link
2025-01-15	[Prestige Maintenance USA]	medusa	Link
2025-01-04	[safecoastseafoods.com]	safepay	Link
2025-01-15	[greyform.sg]	safepay	Link
2025-01-15	[termopuerto.com]	safepay	Link
2025-01-07	[equipo-postal.com]	safepay	Link
2025-01-09	[ddelta.com.mx]	safepay	Link
2025-01-15	[mts.gov.eg]	funksec	Link
2025-01-15	[AKConstructors.com]	ransomhub	Link
2025-01-15	[combinedpoolandspa.com]	kairos	Link
2025-01-15	[Lowe Engineers]	lynx	Link
2025-01-15	[betcllc.com]	apt73	Link
2025-01-15	[Woodport Doors]	lynx	Link
2025-01-15	[barilga.gov.mn]	funksec	Link
2025-01-15	[communisis.com & paragon.world]	lynx	Link
2025-01-15	[anwsd.org]	threeam	Link
2025-01-15	[www.eurocert.pl]	ransomhub	Link
2025-01-15	[jgele.com]	kairos	Link
2025-01-14	[DURAYDUNCAN.COM]	clop	Link
2025-01-14	[Indus Towers]	medusa	Link
2025-01-14	[The Metropolitan Borough of Gateshead]	medusa	Link
2025-01-14	[AVI Southeast]	medusa	Link
2025-01-14	[Boart & Wire]	sarcoma	Link
2025-01-14	[The Chicano Federation]	rhysida	Link
2025-01-14	[udb.net]	ransomhub	Link
2025-01-14	[Beyond79]	akira	Link
2025-01-14	[WPD.WOODPORTDOORS.COM]	lynx	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-01-14	[QualiTech (qualitech.com)]	lynx	Link
2025-01-14	[Kinseth Hospitality Companies]	lynx	Link
2025-01-14	[Douglas County, GA (DDCWSA.COM)]	lynx	Link
2025-01-14	[pittman-construction.com]	lockbit3	Link
2025-01-14	[The University of Oklahoma (ou.edu)]	fog	Link
2025-01-14	[SciTech Services, Inc.]	fog	Link
2025-01-14	[Buttery (butterycompany.com)]	fog	Link
2025-01-14	[Moinho Globo Alimentos]	akira	Link
2025-01-14	[PJ's Rebar]	akira	Link
2025-01-14	[Union Studio]	akira	Link
2025-01-14	[Wynnewood High School]	8base	Link
2025-01-14	[Moraviakov s.r.o.]	8base	Link
2025-01-14	[Bring Solution]	8base	Link
2025-01-14	[Gebäudereinigungsakademie]	8base	Link
2025-01-14	[Thilges & Bernhardt, Attorneys at Law]	qilin	Link
2025-01-14	[Clnica CES]	qilin	Link
2025-01-14	[bluai.ai]	funksec	Link
2025-01-14	[Sharm Reef Hotel]	spacebears	Link
2025-01-14	[Intelservice.com]	ransomhub	Link
2025-01-14	[Solaris Pharma]	everest	Link
2025-01-14	[Onecare]	incransom	Link
2025-01-14	[Findhelp Information Services]	incransom	Link
2025-01-14	[Biomedical Caledonia Medical Laboratory (calmedlab.local)]	incransom	Link
2025-01-14	[Imperial Valley Respite (ivrespite.com)]	incransom	Link
2025-01-14	[Riverina Medical]	incransom	Link
2025-01-14	[Spectrum]	incransom	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-01-13	[SERGAS Group]	lynx	Link
2025-01-13	[Nash Brothers Construction (nashdom.local)]	lynx	Link
2025-01-13	[PHG CPAs (bushman.biz)]	lynx	Link
2025-01-13	[Browdy (bl.local)]	lynx	Link
2025-01-13	[Novati Constructions]	lynx	Link
2025-01-13	[viacaojacarei.com.br]	lockbit3	Link
2025-01-13	[gelco-s-a.com.br]	lockbit3	Link
2025-01-13	[nicatel.com.uy]	lockbit3	Link
2025-01-13	[lamejor.com.co]	lockbit3	Link
2025-01-13	[candelasyasociados.es]	lockbit3	Link
2025-01-13	[atpformosa.gob.ar]	lockbit3	Link
2025-01-13	[oyolasvegas.com]	lockbit3	Link
2025-01-13	[Welcomehallmission.com]	everest	Link
2025-01-13	[PT PINS Indonesia]	dragonforce	Link
2025-01-13	[Delap & Waller]	lynx	Link
2025-01-13	[Conad (conad.lan)]	lynx	Link
2025-01-13	[healthcarewithinreach.org]	ransomhub	Link
2025-01-13	[mymobileforms app]	funksec	Link
2025-01-13	[kuzstu-nf.ru]	funksec	Link
2025-01-13	[telering.de]	lockbit3	Link
2025-01-13	[mi.edu]	ransomhub	Link
2025-01-13	[linxe.com]	funksec	Link
2025-01-13	[zapopan.gob.mx]	funksec	Link
2025-01-12	[wissenhive.com]	funksec	Link
2025-01-11	[Jim Thompson]	lynx	Link
2025-01-11	[Astaphans]	lynx	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-01-11	[pleasantsconstruction.com]	qilin	Link
2025-01-11	[T. Hasegawa USA]	hunters	Link
2025-01-11	[Barber Specialties]	hunters	Link
2025-01-11	[Costex]	hunters	Link
2025-01-11	[Patriarche Office of Architecture]	hunters	Link
2025-01-11	[COROB]	hunters	Link
2025-01-11	[RocSearch]	hunters	Link
2025-01-11	[Unisource Information Services]	hunters	Link
2025-01-11	[seocommarrakech.com]	funksec	Link
2025-01-11	[schuff.com]	blackbasta	Link
2025-01-11	[granbyindustries.com]	blackbasta	Link
2025-01-11	[plasmatherm.com]	blackbasta	Link
2025-01-11	[arunestates.co.uk]	blackbasta	Link
2025-01-11	[brachot.com]	blackbasta	Link
2025-01-11	[avril.ca]	blackbasta	Link
2025-01-11	[migonline.com]	blackbasta	Link
2025-01-11	[bnext.nl]	blackbasta	Link
2025-01-11	[EKOMERCIO.COM]	clop	Link
2025-01-10	[Peikko]	akira	Link
2025-01-10	[Sheyenne Tooling & Manufacturing]	sarcoma	Link
2025-01-10	[amerplumb.com]	ransomhub	Link
2025-01-10	[Ichikawa North America Corporation]	akira	Link
2025-01-10	[Qualinet]	rhysida	Link
2025-01-10	[www.wisesocon.com]	ransomhub	Link
2025-01-10	[Thomas J. Henry Law]	akira	Link
2025-01-10	[Capesesp]	akira	Link
2025-01-10	[Metalmatrix Clamps]	akira	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-01-10	[xtremmedia.com]	ransomhub	Link
2025-01-10	[OmniRide (omniride.com)]	fog	Link
2025-01-10	[Evidn]	everest	Link
2025-01-10	[EVAS Group]	ElDorado	Link
2025-01-09	[depewgillen.com]	incransom	Link
2025-01-09	[castlehillha.co.uk]	ransomhub	Link
2025-01-09	[drive-lines.com]	ransomhub	Link
2025-01-09	[pnp.co.za]	apt73	Link
2025-01-09	[Rent-2-Own]	medusa	Link
2025-01-09	[alansarioman.com]	embargo	Link
2025-01-09	[gags.gov.eg]	funksec	Link
2025-01-09	[mindev.gov.gr]	funksec	Link
2025-01-09	[Northern Lights Electric]	akira	Link
2025-01-09	[Chain And Rope Suppliers LTD]	akira	Link
2025-01-09	[Huntington Hotel Group]	termite	Link
2025-01-09	[Galfer]	akira	Link
2025-01-09	[Permoda]	akira	Link
2025-01-09	[Fukoku Co. Ltd.]	spacebears	Link
2025-01-09	[bendixengineering]	medusalocker	Link
2025-01-09	[carc.gov.jo]	funksec	Link
2025-01-08	[kingpower.com]	abyss	Link
2025-01-08	[Press Color]	akira	Link
2025-01-08	[Surface Combustion]	akira	Link
2025-01-08	[Slawson Companies]	akira	Link
2025-01-08	[sahpetrol.com.tr]	ransomhub	Link
2025-01-08	[Youth Eastside Services]	incransom	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-01-08	[EBL PARTNERS (construction interiors), Florida]	spacebears	spacebears
2025-01-08	[General Digital]	spacebears	Link
2025-01-08	[General Digital CRM]	spacebears	Link
2025-01-07	[ndceg.com]	funksec	Link
2025-01-07	[astaphans.com]	lynx	Link
2025-01-07	[jimthompson.com]	lynx	Link
2025-01-07	[Saint-Bar (saintbar.be)]	fog	Link
2025-01-07	[Arrotex Pharmaceuticals]	morpheus	Link
2025-01-07	[Pus Gmbh]	morpheus	Link
2025-01-07	[Drivestream]	akira	Link
2025-01-07	[Drywall Partitions]	akira	Link
2025-01-07	[D-7 Roofing]	lynx	Link
2025-01-07	[Bergström Wines]	8base	Link
2025-01-07	[Sunflower Medical Group]	rhysida	Link
2025-01-07	[senergy.net]	funksec	Link
2025-01-07	[HECTARE]	8base	Link
2025-01-07	[Lake Shore Public Schools]	8base	Link
2025-01-07	[SPORT BOUTIQ]	8base	Link
2025-01-07	[CED Solutions Computer IT Training Centers]	8base	Link
2025-01-07	[Weininger Metall System GmbH]	8base	Link
2025-01-07	[Omnitravel]	8base	Link
2025-01-07	[ASCOM S.p.A.]	8base	Link
2025-01-06	[VELSOL.COM]	cllop	Link
2025-01-06	[WSINC.COM]	cllop	Link
2025-01-06	[Maverick Constructors]	akira	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-01-06	[yoniot.cn]	darkvault	Link
2025-01-06	[Los Andes]	akira	Link
2025-01-06	[Bluegrass Ingredients]	akira	Link
2025-01-06	[Action Imports]	akira	Link
2025-01-06	[Gunnar Prefab]	akira	Link
2025-01-06	[molars.co.ke]	ransomhub	Link
2025-01-05	[Hunter Taubman Fischer & Li]	lynx	Link
2025-01-05	[ribernuez.com]	funksec	Link
2025-01-05	[bayan-ulgii.cfga.gov.mn]	funksec	Link
2025-01-04	[gsw.co.in]	funksec	Link
2025-01-04	[technotouch.co]	funksec	Link
2025-01-04	[Inventory Management and Counting Solutions]	ElDorado	Link
2025-01-04	[HIDROCARBUROS ARGENTINOS S.A.]	ElDorado	Link
2025-01-04	[Perú Controls S.A.C.]	ElDorado	Link
2025-01-04	[Auxis]	apos	Link
2025-01-04	[Montreal North]	rhysida	Link
2025-01-04	[maxvaluecredits.com]	qilin	Link
2025-01-03	[ISOR]	cicada3301	Link
2025-01-03	[Nikki-Universal Co Ltd]	hunters	Link
2025-01-03	[Lyons Specialty Co.]	8base	Link
2025-01-03	[SolGeo AG Baugelogie and Geotechnik]	8base	Link
2025-01-03	[Grupo Buddemeyer]	8base	Link
2025-01-03	[VOLTAIRE AVOCATS]	8base	Link
2025-01-03	[Jay Enn Corporation]	8base	Link
2025-01-03	[Tarnaise des Panneaux SAS]	8base	Link
2025-01-03	[Carrollton Orthopaedic Clinic]	8base	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-01-02	[confluxhr.com]	darkvault	Link
2025-01-01	[scps.mp.gov.in]	funksec	Link
2025-01-01	[Kitevuc - Equipamentos E Veiculos Utilitários E Comerciais]	ciphbit	Link
2025-01-01	[lianbeng.sg]	ransomhub	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.