Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250118

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

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

—

Webkonferenzen: Zoom Workplace Apps mit Sicherheitslücken

In den Workplace Apps und im Jenkins Plug-in von Zoom klaffen Sicherheitslücken. Updates zum Abdichten der Lecks stehen bereit.

- Link

—

Adobe-Patchday: Gefährliche Sicherheitslücken in Photoshop & Co. geschlossen

Angreifer können Adobe-Anwendungen attackieren, um Computer zu kompromittieren. Sicherheitsupdates schaffen Abhilfe.

- Link

—

Microsoft-Patchday: Angreifer nutzen drei Lücken in Hyper-V aus

Microsoft hat wichtige Sicherheitsupdates unter anderem für Azure, Office und Windows veröffentlicht. Es laufen bereits Attacken.

- Link

—

Jetzt patchen! Attacken auf BeyondTrust PRA/RS und Qlik Sense

Die US-Sicherheitsbehörde CISA warnt vor Attacken auf Fernzugriffssoftware von BeyondTrust und die Datenanalyselösung Qlik Sense Enterprise.

- 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	0.926200000	0.992450000	Link
CVE-2023-6895	0.929940000	0.992800000	Link
CVE-2023-6553	0.959610000	0.996240000	Link
CVE-2023-6019	0.942220000	0.993960000	Link
CVE-2023-6018	0.926470000	0.992480000	Link
CVE-2023-52251	0.953810000	0.995340000	Link
CVE-2023-4966	0.952900000	0.995240000	Link
CVE-2023-49103	0.952840000	0.995230000	Link
CVE-2023-48795	0.948600000	0.994650000	Link
CVE-2023-48788	0.967910000	0.997950000	Link
CVE-2023-47246	0.960960000	0.996460000	Link
CVE-2023-46805	0.964050000	0.997090000	Link
CVE-2023-46747	0.972880000	0.999350000	Link
CVE-2023-46604	0.970820000	0.998790000	Link
CVE-2023-4542	0.929810000	0.992780000	Link
CVE-2023-43208	0.974800000	0.999850000	Link
CVE-2023-43177	0.966220000	0.997550000	Link
CVE-2023-42793	0.974850000	0.999870000	Link
CVE-2023-4220	0.954100000	0.995400000	Link
CVE-2023-39143	0.920920000	0.992060000	Link
CVE-2023-38035	0.972090000	0.999140000	Link
CVE-2023-35813	0.921490000	0.992120000	Link
CVE-2023-3519	0.964000000	0.997070000	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	0.971310000	0.998910000	Link
CVE-2023-34105	0.948800000	0.994670000	Link
CVE-2023-34039	0.958830000	0.996160000	Link
CVE-2023-3368	0.937700000	0.993510000	Link
CVE-2023-33246	0.973200000	0.999480000	Link
CVE-2023-32315	0.970190000	0.998560000	Link
CVE-2023-32235	0.929990000	0.992810000	Link
CVE-2023-30625	0.939600000	0.993720000	Link
CVE-2023-30013	0.968230000	0.998040000	Link
CVE-2023-29298	0.971730000	0.999010000	Link
CVE-2023-28432	0.931990000	0.992980000	Link
CVE-2023-28343	0.966300000	0.997570000	Link
CVE-2023-28121	0.910260000	0.991250000	Link
CVE-2023-27524	0.972590000	0.999240000	Link
CVE-2023-27372	0.973390000	0.999530000	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	0.995320000	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	0.964740000	0.997210000	Link
CVE-2023-22527	0.972290000	0.999180000	Link
CVE-2023-22518	0.969410000	0.998340000	Link
CVE-2023-22515	0.969730000	0.998440000	Link
CVE-2023-20887	0.972060000	0.999110000	Link
CVE-2023-1671	0.957150000	0.995850000	Link
CVE-2023-0669	0.971270000	0.998900000	Link
CVE-2023-0297	0.948640000	0.994650000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 17 Jan 2025

[UPDATE] [hoch] Rsync: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Rsync ausnutzen, um vertrauliche Informationen preiszugeben, sich erhöhte Rechte zu verschaffen und Daten zu manipulieren.

- Link

—

Fri, 17 Jan 2025

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in GIMP ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Fri, 17 Jan 2025

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache Commons ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 17 Jan 2025

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Python ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Fri, 17 Jan 2025

[UPDATE] [hoch] VPN Clients / DHCP: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein Angreifer aus einem angrenzenden Netzwerk kann eine Schwachstelle in VPN-Clients ausnutzen, die auf DHCP konfigurierten Systemen laufen, um den Datenverkehr umzuleiten.

- Link

—

Fri, 17 Jan 2025

[UPDATE] [hoch] Moxa Router: Mehrere Schwachstellen ermöglichen Dateimanipulation und Codeausführung

Ein entfernter anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Moxa Router ausnutzen, um Dateien zu manipulieren und beliebigen Code auszuführen.

- Link

—

Fri, 17 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

—

Fri, 17 Jan 2025

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

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

- Link

—

Fri, 17 Jan 2025

[UPDATE] [hoch] Apache Tomcat: Mehrere Schwachstellen

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

- Link

—

Fri, 17 Jan 2025

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

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

- Link

—

Fri, 17 Jan 2025

[UPDATE] [hoch] libxml2: Schwachstelle ermöglicht XXE Angriffe

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in libxml2 ausnutzen, um Dateien zu manipulieren oder einen Denial of Service zu verursachen.

- Link

—

Fri, 17 Jan 2025

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

Ein entfernter, anonymer 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

—

Fri, 17 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

—

Fri, 17 Jan 2025

[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen

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

- Link

—

Thu, 16 Jan 2025

[NEU] [UNGEPATCHT] [hoch] D-LINK Router (DIR-823X): Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in D-LINK DIR-823X Routern ausnutzen,

um einen Denial of Service Angriff durchzuführen.

- Link

—

Thu, 16 Jan 2025

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

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

- Link

—

Thu, 16 Jan 2025

[UPDATE] [hoch] mutt: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in mutt ausnutzen, um beliebigen Programmcode mit Benutzerrechten auszuführen, Angriffe mit nicht näher spezifizierten Auswirkungen oder einen Denial of Service Angriff durchzuführen.

- Link

—

Thu, 16 Jan 2025

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

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Cross-Site-Scripting-Angriff durchzuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen, Dateien zu manipulieren und einen nicht spezifizierten Angriff durchzuführen.

- Link

—

Thu, 16 Jan 2025

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Denial of Service Angriff durchzuführen oder Code auszuführen.

- Link

—

Thu, 16 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

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
1/17/2025	[Progress WhatsUp Gold < 24.0.2 Multiple Vulnerabilities (000273323)]	critical
1/17/2025	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : Apache Commons BCEL vulnerability (USN-7208-1)]	critical
1/17/2025	[Ubuntu 24.10 : HarfBuzz vulnerability (USN-7214-1)]	critical
1/17/2025	[Ubuntu 24.10 : libxml2 vulnerability (USN-7215-1)]	critical
1/17/2025	[Debian dsa-5845 : libtomcat10-embed-java - security update]	critical
1/17/2025	[RockyLinux 8 : raptor2 (RLSA-2025:0314)]	critical
1/17/2025	[Fedora 41 : redict (2025-d6c0319427)]	high
1/17/2025	[SUSE SLES15 Security Update : kernel (Live Patch 13 for SLE 15 SP5) (SUSE-SU-2025:0146-1)]	high
1/17/2025	[Adobe Substance 3D Designer 14.1 Multiple Vulnerabilities (APSB25-06)]	high
1/17/2025	[Adobe Substance 3D Stager 3.1.0 Multiple Vulnerabilities (APSB25-03)]	high
1/17/2025	[RedShift JDBC Driver < 2.1.0.32 (CVE-2024-12744)]	high
1/17/2025	[RedShift Python Connector < 2.1.5 (CVE-2024-12745)]	high
1/17/2025	[Zoom Workplace Desktop App < 6.2.10 Privilege Escalation (ZSB-25006)]	high
1/17/2025	[Ubuntu 20.04 LTS / 22.04 LTS : Python 2.7 vulnerabilities (USN-7212-1)]	high
1/17/2025	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : GIMP DDS Plugin vulnerabilities (USN-7209-1)]	high
1/17/2025	[Ubuntu 22.04 LTS / 24.04 LTS / 24.10 : .NET vulnerabilities (USN-7210-1)]	high

Datum	Schwachstelle	Bewertung
1/17/2025	[SonarSource SonarQube Server < 9.9.5 / 10.x < 10.5 GitHub Integration JWT Exfiltration (CVE-2024-47910)]	high
1/17/2025	[FreeBSD : openvpn – too long a username or password from a client can confuse openvpn servers (47bc292a-d472-11ef-aaab-7d43732cb6f5)]	high
1/17/2025	[RockyLinux 8 : rsync (RLSA-2025:0325)]	high
1/17/2025	[Ivanti Endpoint Manager 2024 - January 2025 Security Update]	high
1/17/2025	[Ivanti Endpoint Manager 2022 SU6 - January 2025 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 vulnerability. 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

“Wed, 15 Jan 2025

ZDI-25-030: Microsoft Office Word DOCX File Parsing Uninitialized Pointer Remote Code Execution Vulnerability

- Link

—

” “Wed, 15 Jan 2025

ZDI-25-029: Microsoft Windows Installer Service Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Wed, 15 Jan 2025

ZDI-25-028: Microsoft Office Word RTF File Parsing Memory Corruption 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
2025-01-13	Aurora Public Schools	[USA]	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-Grupppe	Webseite
2025-01-18	[gonzalesusd.net]	safepay	Link
2025-01-18	[Kassin & Carrow]	lynx	Link
2025-01-17	[Gossett Motor Cars]	lynx	Link
2025-01-17	[nightingalehammerson.org]	kairos	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-01-17	[funkforum]	funksec	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
2025-01-16	[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
2025-01-16	[Access Capital Partners SA]	lynx	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2025-01-15	[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	[betclic.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
2025-01-14	[QualiTech (qualitech.com)]	lynx	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2025-01-13	[SERGAS Group]	lynx	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2025-01-11	[pleasantsconstruction.com]	qilin	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2025-01-10	[xtremmedia.com]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2025-01-08	[EBL PARTNERS (construction	interiors), Florida]	spacebears

Datum	Opfer	Ransomware-Grupppe	Webseite
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	[AAA Environmental]	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]	clop	Link
2025-01-06	[WSINC.COM]	clop	Link
2025-01-06	[Maverick Constructors]	akira	Link
2025-01-06	[A Bar A Ranch]	akira	Link

Datum	Opfer	Ransomware-Grupppe	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-Grupppe	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.