
Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250113



Inhaltsverzeichnis

1 Editorial	2
2 Security-News	3
2.1 Heise - Security-Alert	3
3 Sicherheitslücken	4
3.1 EPSS	4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit	5
3.2 BSI - Warn- und Informationsdienst (WID)	7
3.3 Sicherheitslücken Meldungen von Tenable	11
4 Aktiv ausgenutzte Sicherheitslücken	12
4.1 Exploits der letzten 5 Tage	12
4.2 0-Days der letzten 5 Tage	17
5 Die Hacks der Woche	20
5.0.1 Gehackt via Nachbar... oder die Palo Alto.	20
6 Cyberangriffe: (Jan)	21
7 Ransomware-Erpressungen: (Jan)	21
8 Quellen	26
8.1 Quellenverzeichnis	26
9 Impressum	27

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

Anonymisierendes Linux: Tails 6.11 stopft kritische Sicherheitslecks

Die Linux-Distribution Tails zum Mitnehmen auf USB-Stick zum anonymen Surfen im Netz schließt mit Version 6.11 kritische Sicherheitslücken.

- [Link](#)

—

Sicherheitsupdates: Angreifer können Netzwerkgeräte mit Junos OS crashen lassen

Netzwerkgeräte wie Switches von Juniper sind verwundbar. Ansatzpunkte sind mehrere Schwachstellen im Betriebssystem Junos OS.

- [Link](#)

—

Migrationstool Palo Alto Expedition gefährdet Netzwerksicherheit

Palo Altos Expedition soll den Umzug von anderen Firewalls vereinfachen. Neue Sicherheitslücken gefährden die Netzwerksicherheit.

- [Link](#)

—

Sicherheitsupdates: Bridge und Switch von HPE Aruba Networking angreifbar

Schwachstellen bedrohen 501 Wireless Client Bridge und Networking CX 10000 Switch Series von HPE Aruba. Exploitcode ist in Umlauf.

- [Link](#)

—

CMS: Updates stopfen Sicherheitslecks in Progress Sitefinity

Im CMS Sitefinity von Progress haben die Entwickler zwei als hochriskant eingestufte Sicherheitslücken entdeckt. Updates dichten sie ab.

- [Link](#)

—

Kein Patch für Lücke in WordPress-Plug-in Fancy Product Designer in Sicht

Es können Attacken auf Onlineshops auf WordPress-Basis mit Fancy Product Designer bevorstehen.

- [Link](#)

—

Ivanti Connect Secure: Angreifer attackieren kritische Sicherheitslücke

Ivanti warnt vor aktiven Angriffen auf Ivanti Secure Connect-Systeme. Durch Codeschmuggel können Netzwerke kompromittiert werden.

- [Link](#)

—

IBM stopft Sicherheitslecks in Cognos Controller

IBM hat Updates für Cognos Controller sowie Controller veröffentlicht. Sie schließen unter anderem Schwachstellen mit hohem Risiko.

- [Link](#)

US-Sicherheitsbehörde warnt vor Attacken auf MiCollab und WebLogic Server

Admins sollten ihre Systeme mit Mittel- und Oracle-Software gegen derzeit laufende Angriffe rüsten.

- [Link](#)

Webbrowser: Chrome- und Firefox-Updates stopfen teils hochriskante Lücken

Neue Versionen von Google Chrome und Mozilla Firefox schließen Sicherheitslücken in den Webbrowsern. Einige gelten als hochriskant.

- [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	0.992420000	Link
CVE-2023-6895	0.929940000	0.992770000	Link
CVE-2023-6553	0.958240000	0.996010000	Link
CVE-2023-6019	0.942220000	0.993950000	Link
CVE-2023-6018	0.926470000	0.992450000	Link
CVE-2023-52251	0.953810000	0.995350000	Link
CVE-2023-4966	0.952900000	0.995260000	Link
CVE-2023-49103	0.952840000	0.995240000	Link
CVE-2023-48795	0.948600000	0.994630000	Link
CVE-2023-48788	0.967910000	0.997960000	Link
CVE-2023-47246	0.960960000	0.996470000	Link
CVE-2023-46805	0.964050000	0.997100000	Link
CVE-2023-46747	0.973210000	0.999460000	Link
CVE-2023-46604	0.970820000	0.998760000	Link
CVE-2023-4542	0.929810000	0.992760000	Link
CVE-2023-43208	0.974800000	0.999850000	Link
CVE-2023-43177	0.966220000	0.997560000	Link
CVE-2023-42793	0.974850000	0.999860000	Link
CVE-2023-4220	0.954100000	0.995410000	Link
CVE-2023-39143	0.922430000	0.992130000	Link
CVE-2023-38035	0.972090000	0.999130000	Link
CVE-2023-35813	0.921490000	0.992060000	Link
CVE-2023-3519	0.964000000	0.997090000	Link
CVE-2023-35082	0.960390000	0.996370000	Link
CVE-2023-35078	0.969220000	0.998300000	Link
CVE-2023-34993	0.968280000	0.998050000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34634	0.908890000	0.991160000	Link
CVE-2023-34362	0.971310000	0.998890000	Link
CVE-2023-34105	0.945570000	0.994290000	Link
CVE-2023-34039	0.958830000	0.996160000	Link
CVE-2023-3368	0.937700000	0.993480000	Link
CVE-2023-33246	0.973200000	0.999450000	Link
CVE-2023-32315	0.970610000	0.998700000	Link
CVE-2023-32235	0.929990000	0.992770000	Link
CVE-2023-30625	0.939600000	0.993700000	Link
CVE-2023-30013	0.968230000	0.998040000	Link
CVE-2023-29298	0.971730000	0.999010000	Link
CVE-2023-28432	0.931990000	0.992950000	Link
CVE-2023-28343	0.966300000	0.997580000	Link
CVE-2023-28121	0.924130000	0.992250000	Link
CVE-2023-27524	0.972590000	0.999250000	Link
CVE-2023-27372	0.973390000	0.999520000	Link
CVE-2023-27350	0.968700000	0.998160000	Link
CVE-2023-26469	0.950080000	0.994870000	Link
CVE-2023-26035	0.969170000	0.998280000	Link
CVE-2023-25717	0.953520000	0.995330000	Link
CVE-2023-25194	0.960710000	0.996430000	Link
CVE-2023-2479	0.966080000	0.997530000	Link
CVE-2023-24489	0.972450000	0.999230000	Link
CVE-2023-23752	0.936010000	0.993290000	Link
CVE-2023-23333	0.964740000	0.997240000	Link
CVE-2023-22527	0.972290000	0.999180000	Link
CVE-2023-22518	0.969410000	0.998330000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-22515	0.969730000	0.998440000	Link
CVE-2023-20887	0.972060000	0.999110000	Link
CVE-2023-1671	0.957150000	0.995840000	Link
CVE-2023-0669	0.971270000	0.998880000	Link
CVE-2023-0297	0.948640000	0.994640000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 10 Jan 2025

[UPDATE] [hoch] Drupal: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Drupal ausnutzen, um Sicherheitsmaßnahmen zu umgehen, einen Cross-Site-Scripting-Angriff durchzuführen oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Fri, 10 Jan 2025

[UPDATE] [hoch] Drupal: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Drupal ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen, beliebigen Code auszuführen und nicht spezifizierte Auswirkungen zu verursachen.

- [Link](#)

—

Fri, 10 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, 10 Jan 2025

[UPDATE] [hoch] Paessler PRTG: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein Angreifer aus einem angrenzenden Netzwerk kann eine Schwachstelle in Paessler PRTG ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Fri, 10 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, 10 Jan 2025

[UPDATE] [hoch] Drupal: Mehrere Schwachstellen ermöglichen Codeausführung und Cross Site Scripting

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Drupal ausnutzen, um beliebigen Programmcode auszuführen und einen Cross-Site-Scripting-Angriff durchzuführen.

- [Link](#)

—

Fri, 10 Jan 2025

[UPDATE] [hoch] Drupal: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Drupal ausnutzen, um vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand zu erzeugen, Sicherheitsmaßnahmen zu umgehen oder XSS-Angriffe durchzuführen.

- [Link](#)

—

Fri, 10 Jan 2025

[UPDATE] [hoch] Drupal: Mehrere Schwachstellen

Ein anonymer Angreifer kann mehrere Schwachstellen in Drupal ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Fri, 10 Jan 2025

[UPDATE] [hoch] Red Hat OpenShift Container Platform: Mehrere Schwachstellen

Ein entfernter anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat OpenShift Container Platform ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen, Dateien und Daten zu manipulieren oder Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

—

Fri, 10 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, 10 Jan 2025

[UPDATE] [hoch] WebKit: Mehrere Schwachstellen ermöglichen Cross-Site Scripting und Code-Ausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in WebKit ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen und beliebigen Code auszuführen.

- [Link](#)

—

Fri, 10 Jan 2025

[UPDATE] [hoch] Drupal: Mehrere Schwachstellen ermöglichen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Drupal ausnutzen, um Sicherheitsmaßnahmen zu umgehen, einen Cross-Site-Scripting-Angriff durchzuführen oder einen unspezifischen Angriff auszuführen.

- [Link](#)

—

Thu, 09 Jan 2025

[UPDATE] [hoch] Red Hat OpenShift: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial of Service Angriff durchzuführen oder beliebigen Programmcode auszuführen.

- [Link](#)

—

Thu, 09 Jan 2025

[UPDATE] [hoch] Red Hat OpenShift: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um Dateien zu manipulieren, einen Denial-of-Service-Zustand zu verursachen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, seine Privilegien zu erweitern oder um weitere nicht spezifizierte Angriffe auszuführen.

- [Link](#)

—

Thu, 09 Jan 2025

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PaloAlto Networks Expedition ausnutzen, um Daten zu manipulieren, Informationen offenzulegen, einen Cross Site Scripting Angriff durchzuführen, oder Befehle auszuführen.

- [Link](#)

—

Thu, 09 Jan 2025

[UPDATE] [hoch] Google Chrome: Schwachstelle ermöglicht Codeausführung

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

- [Link](#)

—

Thu, 09 Jan 2025

[NEU] [hoch] Juniper JUNOS: Mehrere Schwachstellen ermöglichen Denial of Service und Informationsoffenlegung

Ein Angreifer kann mehrere Schwachstellen in Juniper JUNOS ausnutzen, um einen Denial of Service Angriff durchzuführen und um vertrauliche Informationen preiszugeben.

- [Link](#)

—

Thu, 09 Jan 2025

[UPDATE] [hoch] Ruby: Schwachstelle ermöglicht Codeausführung

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

- [Link](#)

—

Thu, 09 Jan 2025

[UPDATE] [hoch] Ruby: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Ruby ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service zu verursachen.

- [Link](#)

—

Thu, 09 Jan 2025

[UPDATE] [hoch] Net-SNMP: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein Angreifer kann mehrere Schwachstellen in Net-SNMP ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
1/10/2025	[IBM DB2 SEoL (9.1.x)]	critical
1/10/2025	[Wireshark SEoL (1.5.x <= x <= 1.6.x)]	critical
1/10/2025	[IBM DB2 SEoL (7.2.x)]	critical
1/10/2025	[IBM DB2 SEoL (9.5.x)]	critical
1/10/2025	[Wireshark SEoL (1.10.x)]	critical
1/10/2025	[IBM DB2 SEoL (<= 7.1.x)]	critical
1/10/2025	[Mozilla Firefox SEoL (81.x)]	high
1/10/2025	[Mozilla Firefox SEoL (97.x)]	high
1/10/2025	[Mozilla Firefox ESR SEoL (17.x)]	high
1/10/2025	[Mozilla Firefox ESR SEoL (68.x)]	high
1/10/2025	[Mozilla Firefox SEoL (52.x)]	high
1/10/2025	[Mozilla Firefox SEoL (79.x)]	high
1/10/2025	[Mozilla Firefox SEoL (37.x)]	high
1/10/2025	[Mozilla Firefox SEoL (24.x)]	high
1/10/2025	[Mozilla Firefox SEoL (20.x)]	high
1/10/2025	[Mozilla Firefox SEoL (98.x)]	high
1/10/2025	[Mozilla Firefox SEoL (9.x)]	high
1/10/2025	[Mozilla Firefox SEoL (1.x)]	high
1/10/2025	[Mozilla Firefox SEoL (3.x)]	high
1/10/2025	[Mozilla Firefox SEoL (31.x)]	high
1/10/2025	[Mozilla Firefox SEoL (54.x)]	high
1/10/2025	[Mozilla Firefox SEoL (38.x)]	high
1/10/2025	[Mozilla Firefox SEoL (48.x)]	high
1/10/2025	[Mozilla Firefox SEoL (74.x)]	high

Datum	Schwachstelle	Bewertung
1/10/2025	[Mozilla Firefox SEoL (69.x)]	high
1/10/2025	[Mozilla Firefox ESR SEoL (78.x)]	high
1/10/2025	[Mozilla Firefox SEoL (93.x)]	high
1/10/2025	[Mozilla Firefox SEoL (56.x)]	high
1/10/2025	[Mozilla Firefox SEoL (23.x)]	high
1/10/2025	[Mozilla Firefox ESR SEoL (10.x)]	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

“Sun, 12 Jan 2025

ZDI-25-027: (Pwn2Own) Google Chrome VideoFrame Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

—

” “Fri, 10 Jan 2025

ZDI-25-026: Mintty Path Conversion Improper Input Validation Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 09 Jan 2025

ZDI-25-025: Avira Prime System Speedup Service Link Following Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Thu, 09 Jan 2025

ZDI-25-024: Avira Prime System Speedup Service Link Following Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Thu, 09 Jan 2025

ZDI-25-023: Avira Prime System Speedup Service Link Following Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Thu, 09 Jan 2025

ZDI-25-022: Apple macOS libFontValidation Font Glyph YCoordinate Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 09 Jan 2025

ZDI-25-021: Apple macOS libFontValidation Font Glyph Flags Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 09 Jan 2025

ZDI-25-020: Apple macOS libFontValidation post Table Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 09 Jan 2025

ZDI-25-019: Apple macOS libFontValidation loca Table Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 09 Jan 2025

ZDI-25-018: Apple macOS libFontValidation Font Header Name Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 09 Jan 2025

ZDI-25-017: Apple macOS libFontValidation kern Table Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 09 Jan 2025

ZDI-25-016: Apple macOS CoreText Font Ligature Caret List Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 09 Jan 2025

ZDI-25-015: Apple macOS CoreText Font Ligature Caret List Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 09 Jan 2025

ZDI-25-014: SonicWALL NSv setSshdConfig Exposed Dangerous Function Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Thu, 09 Jan 2025

ZDI-25-013: SonicWALL NSv SSH Management Server-Side Request Forgery Vulnerability

- [Link](#)

—

” “Thu, 09 Jan 2025

ZDI-25-012: SonicWALL NSv Authentication Bypass Vulnerability

- [Link](#)

—

” “Thu, 09 Jan 2025

ZDI-25-011: SonicWALL NSv Cryptographically Weak PRNG Authentication Bypass Vulnerability

- [Link](#)

—

” “Thu, 09 Jan 2025

ZDI-25-010: Redis Stack Lua Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 09 Jan 2025

ZDI-25-009: Redis Stack RedisBloom Integer Overflow 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
2025-01-08	Office of Geodesy, Cartography and Cadastre of the Slovak Republic (UGKK)	[SVK]	Link
2025-01-08	Prefeitura de Sarapuí	[BRA]	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
2025-01-03	La Police de Kingston	[CAN]	Link

7 Ransomware-Erpressungen: (Jan)

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-01-12	[behind funksec]	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
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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	Link
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[YorkTest Laboratories]	qilin	Link
2025-01-04	[www.smawins.com]	qilin	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
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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.