

Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250104



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	18
5.0.1 Gehackt via Nachbar... oder die Palo Alto.	18
6 Cyberangriffe: (Jan)	19
7 Ransomware-Erpressungen: (Jan)	19
8 Quellen	19
8.1 Quellenverzeichnis	19
9 Impressum	21

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

Authentifizierung von IBM Db2 unter Cloud Pak for Data umgehbar

IBMs Datenbanksysteme Db2 und Db2 Warehouse sind unter der Daten- und KI-Plattform Cloud Pak for Data attackierbar.

- [Link](#)

—

Sicherheitslücke: Angreifer können Palo-Alto-Firewalls in Wartungsmodus schicken

Eine Schwachstelle im Firewall-Betriebssystem PAN-OS kann Netzwerke gefährden. Sicherheitspatches stehen bereit.

- [Link](#)

—

Kein Sicherheitspatch in Sicht: Paessler PRTG Network Monitor ist attackierbar

Die Netzwerk-Monitoring-Software Paessler PRTG ist verwundbar. Wann der Hersteller die Software absichert, ist bislang unbekannt.

- [Link](#)

—

Kritische Sicherheitslücken bedrohen Sophos-Firewalls

Es sind wichtige Sicherheitsupdates für Firewalls von Sophos erschienen. Mit den Standardeinstellungen installieren sie sich automatisch.

- [Link](#)

—

Fortinet Wireless Manager: Informationen zu kritischer Lücke zurückgehalten

Angreifer konnten Fortinet Wireless Manager attackieren und Admins-Sessions kapern. Das Netzwerkmanagementtool war über mehrere Monate verwundbar.

- [Link](#)

—

Kritische Lücke in BeyondTrust Privileged Remote Access und Remote Support

In aktuellen Versionen von BeyondTrust Privileged Remote Access und Remote Support haben die Entwickler eine gefährliche Schwachstelle geschlossen.

- [Link](#)

—

Windows-Sicherheitslösung Trend Micro Apex One als Einfallstor für Angreifer

Angreifer können an mehreren Sicherheitslücken in Trend Micro Apex One ansetzen. Sicherheitsupdates sind verfügbar.

- [Link](#)

Jetzt patchen! Angreifer nutzen kritische Sicherheitslücke in Apache Struts aus

Die Uploadfunktion von Apache Struts ist fehlerhaft und Angreifer können Schadcode hochladen. Sicherheitsforscher warnen vor Attacken.

- [Link](#)

Foxit PDF Editor und Reader: Attacken über präparierte PDF-Dateien möglich

PDF-Anwendungen von Foxit sind unter macOS und Windows verwundbar. Sicherheitsupdates stehen bereit.

- [Link](#)

CyberPanel: Angreifer können Schadcode einschleusen

In der Server-Verwaltungssoftware CyberPanel wurden zwei Schwachstellen entdeckt. Sie erlauben Angreifern das Einschleusen beliebigen Codes.

- [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	0.916790000	0.991600000	Link
CVE-2023-6895	0.929940000	0.992740000	Link
CVE-2023-6553	0.958240000	0.996000000	Link
CVE-2023-6019	0.942220000	0.993920000	Link
CVE-2023-6018	0.926470000	0.992420000	Link
CVE-2023-52251	0.954310000	0.995420000	Link
CVE-2023-4966	0.952900000	0.995230000	Link
CVE-2023-49103	0.950490000	0.994920000	Link
CVE-2023-48795	0.948600000	0.994620000	Link
CVE-2023-48788	0.967260000	0.997790000	Link
CVE-2023-47246	0.960960000	0.996460000	Link
CVE-2023-46805	0.964050000	0.997110000	Link
CVE-2023-46747	0.973480000	0.999520000	Link
CVE-2023-46604	0.971630000	0.998990000	Link
CVE-2023-4542	0.925090000	0.992310000	Link
CVE-2023-43208	0.975000000	0.999890000	Link
CVE-2023-43177	0.966220000	0.997560000	Link
CVE-2023-42793	0.974850000	0.999860000	Link
CVE-2023-4220	0.954510000	0.995450000	Link
CVE-2023-39143	0.922430000	0.992100000	Link
CVE-2023-38035	0.971600000	0.998980000	Link
CVE-2023-35813	0.919220000	0.991820000	Link
CVE-2023-3519	0.962770000	0.996830000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-35082	0.960390000	0.996350000	Link
CVE-2023-35078	0.967920000	0.997960000	Link
CVE-2023-34993	0.968280000	0.998040000	Link
CVE-2023-34362	0.970610000	0.998680000	Link
CVE-2023-34105	0.945570000	0.994250000	Link
CVE-2023-34039	0.956980000	0.995780000	Link
CVE-2023-3368	0.937700000	0.993430000	Link
CVE-2023-33246	0.973640000	0.999560000	Link
CVE-2023-32707	0.900600000	0.990610000	Link
CVE-2023-32315	0.970610000	0.998690000	Link
CVE-2023-32235	0.929990000	0.992750000	Link
CVE-2023-30625	0.945900000	0.994280000	Link
CVE-2023-30013	0.968230000	0.998030000	Link
CVE-2023-29298	0.971300000	0.998900000	Link
CVE-2023-28432	0.931990000	0.992920000	Link
CVE-2023-28343	0.966300000	0.997580000	Link
CVE-2023-28121	0.924130000	0.992230000	Link
CVE-2023-27524	0.972790000	0.999320000	Link
CVE-2023-27372	0.973390000	0.999510000	Link
CVE-2023-27350	0.968700000	0.998170000	Link
CVE-2023-26469	0.950080000	0.994860000	Link
CVE-2023-26035	0.969170000	0.998300000	Link
CVE-2023-25717	0.953520000	0.995310000	Link
CVE-2023-25194	0.961930000	0.996650000	Link
CVE-2023-2479	0.965350000	0.997380000	Link
CVE-2023-24489	0.972450000	0.999240000	Link
CVE-2023-23752	0.936010000	0.993250000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23333	0.965180000	0.997350000	Link
CVE-2023-22527	0.971530000	0.998960000	Link
CVE-2023-22518	0.970030000	0.998490000	Link
CVE-2023-22515	0.970820000	0.998760000	Link
CVE-2023-20887	0.972060000	0.999110000	Link
CVE-2023-1671	0.956590000	0.995740000	Link
CVE-2023-0669	0.969800000	0.998440000	Link
CVE-2023-0297	0.948640000	0.994630000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 03 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, 03 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, 03 Jan 2025

[NEU] [hoch] Moxa Router: Mehrere Schwachstellen

Ein entfernter, authentisierter oder anonymer Angreifer kann mehrere Schwachstellen in Moxa Router ausnutzen, um Administratorrechte zu erlangen und um beliebige Kommandos auszuführen.

- [Link](#)

—

Fri, 03 Jan 2025

[UPDATE] [hoch] IBM Java: Schwachstelle ermöglicht Codeausführung

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

- [Link](#)

—

Fri, 03 Jan 2025

[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen

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

- [Link](#)

—

Fri, 03 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, 03 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](#)

—

Fri, 03 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](#)

—

Fri, 03 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, 03 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, vertrauliche Informationen offenzulegen und einen Denial-of-Service-Situation zu erzeugen.

- [Link](#)

—

Thu, 02 Jan 2025

[UPDATE] [hoch] Django: Mehrere Schwachstellen

Ein anonym Angreifer kann mehrere Schwachstellen in Django ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder Daten zu manipulieren.

- [Link](#)

—

Thu, 02 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](#)

—

Thu, 02 Jan 2025

[NEU] [hoch] IBM DB2: Mehrere Schwachstellen

Ein entfernter oder lokaler Angreifer kann mehrere Schwachstellen in IBM DB2 on Cloud Pak for Data ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Tue, 31 Dec 2024

[UPDATE] [hoch] Oracle Fusion Middleware: Mehrere Schwachstellen

Ein entfernter, anonym oder authentisierter Angreifer kann mehrere Schwachstellen in Oracle Fusion Middleware ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

—

Tue, 31 Dec 2024

[UPDATE] [hoch] Foxit PDF Editor und Foxit Reader: Mehrere Schwachstellen

Ein authentifizierter Angreifer kann mehrere Schwachstellen in Foxit PDF Editor und Foxit Reader ausnutzen, um seine Privilegien zu erweitern, beliebigen Code auszuführen, vertrauliche Informationen preiszugeben oder Daten zu manipulieren.

- [Link](#)

—

Tue, 31 Dec 2024

[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](#)

—

Tue, 31 Dec 2024

[NEU] [UNGEPATCHT] [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](#)

—

Mon, 30 Dec 2024

[UPDATE] [hoch] Linux-Kernel: Schwachstelle ermöglicht Denial of Service und Privilegienerweiterung

Ein lokaler Angreifer kann eine Schwachstelle im Linux-Kernel ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder seine Privilegien zu erweitern.

- [Link](#)

—

Mon, 30 Dec 2024

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

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

- [Link](#)

—

Mon, 30 Dec 2024

[NEU] [hoch] NetApp Data ONTAP: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in NetApp Data ONTAP ausnutzen, um einen Denial of Service Angriff durchzuführen, vertrauliche Informationen offenzulegen und Daten zu manipulieren.

- [Link](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
12/30/2024	[FreeBSD : Apache Tomcat – RCE due to TOCTOU issue in JSP compilation (ed0a052a-c5e6-11ef-a457-b42e991fc52e)]	critical
1/3/2025	[Debian dla-4008 : linux-config-6.1 - security update]	critical
1/2/2025	[BeyondTrust Remote Support (RS) <= 24.3.1 Multiple Vulnerabilities]	critical
1/2/2025	[BeyondTrust Privileged Remote Access (PRA) <= 24.3.1 Multiple Vulnerabilities]	critical
1/1/2025	[Fedora 40 : libxml2 (2024-9f3765a04b)]	critical
1/1/2025	[RHEL 8 : python36:3.6 (RHSA-2025:0002)]	critical
1/1/2025	[BeyondTrust Privileged Remote Access Unsupported Version Detection]	critical
1/1/2025	[BeyondTrust Remote Support Unsupported Version Detection]	critical
12/31/2024	[Debian dla-4005 : debootstrap - security update]	high
12/31/2024	[Debian dla-4006 : python-django-doc - security update]	high
12/30/2024	[Couchbase 2.x < 7.2.5 Out-of-Bounds]	high
12/30/2024	[Cisco IOS Software Resource Reservation Protocol DoS (cisco-sa-rsvp-dos-OypvgVZf)]	high
12/30/2024	[Cisco IOS XE Software Resource Reservation Protocol DoS (cisco-sa-rsvp-dos-OypvgVZf)]	high
12/30/2024	[Cisco IOS XE Software Protocol Independent Multicast DoS (cisco-sa-pim-APbVfySJ)]	high
1/3/2025	[IBM Cognos Analytics 11.2.x < 11.2.4 FP5 / 12.0.x < 12.0.4 IF1 Multiple Vulnerabilities (7179496)]	high
1/3/2025	[Adobe ColdFusion < 2021.x < 2021u18 / 2023.x < 2023u12 Path Traversal (APSB24-107)]	high
1/3/2025	[ZenML < 0.55.5 Arbitrary File Upload]	high

Datum	Schwachstelle	Bewertung
1/3/2025	[ZenML < 0.56.3 Unpatched Session Expiration Exposure (CVE-2024-4680)]	high
1/2/2025	[Fedora 40 : iwd / libell (2024-0fa283c43a)]	high
1/2/2025	[Cisco IOS XE Software SD Access Fabric Edge Node DoS (cisco-sa-ios-xe-sda-edge-dos-MBcbG9k)]	high
1/2/2025	[CentOS 9 : kernel-5.14.0-547.el9]	high
1/1/2025	[Photon OS 4.0: Squid PHSA-2024-4.0-0726]	high
1/1/2025	[Photon OS 4.0: Cups PHSA-2024-4.0-0726]	high
1/1/2025	[Photon OS 5.0: Rubygem PHSA-2024-5.0-0432]	high
1/1/2025	[Photon OS 5.0: Squid PHSA-2024-5.0-0429]	high
1/1/2025	[Photon OS 4.0: Linux PHSA-2024-4.0-0722]	high
1/1/2025	[Photon OS 4.0: Python3 PHSA-2024-4.0-0704]	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

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
-------	-------	------	-------------

7 Ransomware-Erpressungen: (Jan)

Datum	Opfer	Ransomware-Gruppe	Webseite
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
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.