Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241205

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

Veeam Service Provider Console: Kritische Lücke gefährdet Kunden-Backups

Veeams Backend-as-a-Service- und Disaster-Recovery-as-a-Service-Plattform Service Provider Console ist verwundbar.

- Link

—

Jetzt patchen! Exploit für kritische Lücke in Whatsup Gold in Umlauf

Die Monitoring-Software Whatsup Gold ist verwundbar. Sicherheitsforscher sind nun auf einen Exploit für Schadcode-Attacken gestoßen. Ein Patch ist verfügbar.

- Link

—

Identitätsmanagement: Sicherheitslücke mit Höchstwertung bedroht IdentityIQ

In aktuellen Versionen haben die Entwickler von SailPoint in IdenetityIQ eine kritische Schwachstelle geschlossen.

- Link

—

Patchday: Android 12, 13, 14 und 15 für Schadcode-Attacken anfällig

Angreifer können Androidgeräte auf verschiedene Weise attackieren und sich Zugriff auf Smartphones verschaffen.

- Link

—

Monitoring-Tool Zabbix: Kritische Lücke ermöglicht Kontrollübernahme

Im Open-Source-Monitoring-Tool Zabbix klafft eine kritische SQL-Injection-Lücke. Angreifer können verwundbare Systeme vollständig übernehmen.

- Link

—

Statische Zugangsdaten in IBM Security Verify Access Appliance entdeckt

Angreifer können IBMs Zugriffsmanagementlösung Security Verify Access Appliance unter anderem mit Schadcode attackieren. Ein Sicherheitsupdate steht bereit.

- Link

—

ProFTPD: Angreifer können Rechte ausweiten

In ProFTPD können Angreifer eine Sicherheitslücke missbrauchen, um ihre Rechte im System auszuweiten. Quellcode-Updates stehen bereit.

- Link

—

Jetzt patchen! Attacken auf Filesharingplattform ProjectSend beobachtet

Auch wenn ein Sicherheitspatch für ProjectSend schon länger als ein Jahr verfügbar ist, sind offensichtlich noch unzählige Instanzen verwundbar.

- Link

—

Hochriskante Sicherheitslücke in PostgreSQL: Gitlab patcht (noch) nicht

Eine bekannte Lücke ermöglicht es einfachen Nutzern, in PostgreSQL Befehle einzuschleusen. Ein Update gäbe es. GitLab installiert es bislang nicht.

- Link

—

Sicherheitslecks in Entwicklerwerkzeug Jenkins gestopft

In dem Software-Entwicklungs-Tool Jenkins haben die Entwickler mehrere Sicherheitslücken gefunden. Updates schließen sie.

- 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	0.958030000	0.995190000	Link
CVE-2023-6895	0.936280000	0.992190000	Link
CVE-2023-6553	0.952340000	0.994240000	Link
CVE-2023-6019	0.935090000	0.992040000	Link
CVE-2023-6018	0.916750000	0.990370000	Link
CVE-2023-52251	0.949550000	0.993840000	Link
CVE-2023-4966	0.971030000	0.998310000	Link
CVE-2023-49103	0.948250000	0.993660000	Link
CVE-2023-48795	0.962800000	0.995980000	Link
CVE-2023-47246	0.963300000	0.996100000	Link
CVE-2023-46805	0.957820000	0.995130000	Link
CVE-2023-46747	0.972680000	0.998930000	Link
CVE-2023-46604	0.967810000	0.997320000	Link
CVE-2023-4542	0.941060000	0.992740000	Link
CVE-2023-43208	0.974210000	0.999550000	Link
CVE-2023-43177	0.959840000	0.995440000	Link
CVE-2023-42793	0.971260000	0.998380000	Link
CVE-2023-41265	0.903830000	0.989480000	Link
CVE-2023-39143	0.920260000	0.990660000	Link
CVE-2023-38205	0.953810000	0.994460000	Link
CVE-2023-38203	0.964750000	0.996430000	Link
CVE-2023-38146	0.906640000	0.989670000	Link
CVE-2023-38035	0.974360000	0.999610000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.967890000	0.997350000	Link
CVE-2023-3519	0.965540000	0.996650000	Link
CVE-2023-35082	0.961850000	0.995800000	Link
CVE-2023-35078	0.967840000	0.997330000	Link
CVE-2023-34993	0.972760000	0.998970000	Link
CVE-2023-34634	0.926130000	0.991110000	Link
CVE-2023-34362	0.970200000	0.998050000	Link
CVE-2023-34039	0.929610000	0.991480000	Link
CVE-2023-3368	0.938260000	0.992420000	Link
CVE-2023-33246	0.973150000	0.999100000	Link
CVE-2023-32315	0.973420000	0.999200000	Link
CVE-2023-32235	0.914280000	0.990240000	Link
CVE-2023-30625	0.950240000	0.993940000	Link
CVE-2023-30013	0.968110000	0.997390000	Link
CVE-2023-29300	0.968250000	0.997450000	Link
CVE-2023-29298	0.969330000	0.997730000	Link
CVE-2023-28432	0.906870000	0.989680000	Link
CVE-2023-28343	0.966250000	0.996820000	Link
CVE-2023-28121	0.929810000	0.991510000	Link
CVE-2023-27524	0.970390000	0.998090000	Link
CVE-2023-27372	0.973870000	0.999390000	Link
CVE-2023-27350	0.968620000	0.997530000	Link
CVE-2023-26469	0.957270000	0.995030000	Link
CVE-2023-26360	0.962010000	0.995840000	Link
CVE-2023-26035	0.968960000	0.997610000	Link
CVE-2023-25717	0.949440000	0.993800000	Link
CVE-2023-25194	0.967670000	0.997290000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963800000	0.996220000	Link
CVE-2023-24489	0.972870000	0.998990000	Link
CVE-2023-23752	0.948310000	0.993670000	Link
CVE-2023-23397	0.902750000	0.989410000	Link
CVE-2023-23333	0.963300000	0.996110000	Link
CVE-2023-22527	0.969680000	0.997840000	Link
CVE-2023-22518	0.963030000	0.996050000	Link
CVE-2023-22515	0.973360000	0.999170000	Link
CVE-2023-21839	0.922450000	0.990800000	Link
CVE-2023-21554	0.951950000	0.994160000	Link
CVE-2023-20887	0.968860000	0.997600000	Link
CVE-2023-1698	0.911050000	0.990030000	Link
CVE-2023-1671	0.962610000	0.995920000	Link
CVE-2023-0669	0.972180000	0.998740000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 04 Dec 2024

[UPDATE] [hoch] X.Org X11 und Xming: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in X.Org X11 und Xming ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu erzeugen oder beliebigen Code auszuführen.

- Link

—

Wed, 04 Dec 2024

[UPDATE] [hoch] PostgreSQL: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, Daten zu manipulieren oder vertrauliche Informationen preiszugeben.

- Link

—

Wed, 04 Dec 2024

[NEU] [hoch] Dell NetWorker: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Dell NetWorker ausnutzen, um Informationen offenzulegen.

- Link

—

Wed, 04 Dec 2024

[NEU] [hoch] Synology Router Manager: Schwachstelle ermöglicht Manipulation von Dateien

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Synology Router Manager ausnutzen, um Dateien zu manipulieren.

- Link

—

Wed, 04 Dec 2024

[NEU] [hoch] Veeam Backup & Replication: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Veeam Backup & Replication ausnutzen, um seine Rechte zu erweitern, vertrauliche Informationen preiszugeben und Dateien zu manipulieren.

- Link

—

Wed, 04 Dec 2024

[UPDATE] [hoch] libxml2: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in libxml2 ausnutzen, um einen Denial of Service Angriff durchzuführen oder vertrauliche Daten einsehen.

- Link

—

Wed, 04 Dec 2024

[UPDATE] [hoch] libxml2: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in libxml2 ausnutzen, um einen Denial of Service Angriff durchzuführen oder vertrauliche Informationen erhalten

- Link

—

Wed, 04 Dec 2024

[UPDATE] [hoch] libxml2: Schwachstelle ermöglicht Denial of Service oder Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in libxml2 ausnutzen, um einen Denial of Service Angriff durchzuführen oder um Informationen offenzulegen.

- Link

—

Wed, 04 Dec 2024

[UPDATE] [hoch] Ansible: Mehrere Schwachstellen ermöglichen Ausführen von beliebigem Programmcode

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Ansible ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 04 Dec 2024

[UPDATE] [hoch] libxml2: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in libxml2 ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.

- Link

—

Wed, 04 Dec 2024

[UPDATE] [hoch] libxml2: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in libxml2 ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 04 Dec 2024

[UPDATE] [hoch] libxml2: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein Angreifer kann mehrere Schwachstellen in libxml2 ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Wed, 04 Dec 2024

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

Ein Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, seine Privilegien zu erweitern, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.

- Link

—

Wed, 04 Dec 2024

[UPDATE] [hoch] docker: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Docker ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen,

Sicherheitsmaßnahmen zu umgehen oder Dateien zu manipulieren.
- Link

—

Wed, 04 Dec 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um Sicherheitsvorkehrungen zu umgehen und um Dateien zu manipulieren.
- Link

—

Wed, 04 Dec 2024

[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in AMD Prozessor und AMD Radeon ausnutzen, um beliebigen Programmcode auszuführen, erhöhte Rechte zu erlangen, einen Denial-of-Service-Zustand zu erzeugen, Daten zu manipulieren, Sicherheitsmaßnahmen zu umgehen und vertrauliche Informationen preiszugeben.
- Link

—

Wed, 04 Dec 2024

[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

—

Wed, 04 Dec 2024

[UPDATE] [hoch] Microsoft Entwicklerwerkzeuge: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein Angreifer kann mehrere Schwachstellen in Microsoft Visual Studio 2015, Microsoft Visual Studio 2017, Microsoft Visual Studio Code, Microsoft .NET Framework, Microsoft Visual Studio 2019, Microsoft Visual Studio 2022 und Microsoft Visual C++ ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen und einen Denial-of-Service-Zustand zu erzeugen.
- Link

—

Wed, 04 Dec 2024

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PHP ausnutzen, um vertrauliche Informationen preiszugeben, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu

erzeugen und einen Spoofing-Angriff durchzuführen.
- Link

—

Wed, 04 Dec 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen preiszugeben, Sicherheitsmaßnahmen zu umgehen oder Cross-Site-Scripting- oder Spoofing-Angriffe durchzuführen.
- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
12/4/2024	[Schneider Electric IONXXXX Series Power Meter Improper Access Control (CVE-2016-5815)]	critical
12/4/2024	[Cisco NX-OS Improper Restriction of Operations within the Bounds of a Memory Buffer (CVE-2016-1453)]	critical
12/4/2024	[Dahua Technology Co., Ltd Digital Video Recorders and IP Cameras Password in Configuration File (CVE-2017-7925)]	critical
12/4/2024	[Cisco Unified IP Phone Use of Hard-coded Credentials (CVE-2007-1063)]	critical
12/4/2024	[Cisco Small Business Improper Restriction of Operations within the Bounds of a Memory Buffer (CVE-2017-12259)]	high
12/4/2024	[Cisco NX-OS Double Free (CVE-2018-0102)]	high
12/4/2024	[Cisco IOS Improper Input Validation (CVE-2016-1409)]	high
12/4/2024	[Cisco IP Phone 7920 SNMP Information Disclosure (CVE-2005-3803)]	high

Datum	Schwachstelle	Bewertung
12/4/2024	[Cisco NX-OS Permissions, Privileges, and Access Controls (CVE-2015-4234)]	high
12/4/2024	[Cisco Unified Computing System Resource Management Errors (CVE-2015-0718)]	high
12/4/2024	[Meinberg NTP Permissions, Privileges, and Access Controls (CVE-2016-3989)]	high
12/4/2024	[Cisco Application Policy Infrastructure Permissions, Privileges, and Access Controls (CVE-2015-4235)]	high
12/4/2024	[Dell 3000cn Permissions, Privileges, and Access Controls (CVE-2006-2112)]	high
12/4/2024	[Phoenix Contact ILC PLCs Denial of Service (CVE-2021-33541)]	high
12/4/2024	[Cisco NX-OS OS Command Injection (CVE-2012-4075)]	high
12/4/2024	[Meinberg NTP Improper Restriction of Operations within the Bounds of a Memory Buffer (CVE-2016-3962)]	high
12/4/2024	[Dahua Technology Co., Ltd Digital Video Recorders and IP Cameras Use of Password Hash Instead of Password For Authentication (CVE-2017-7927)]	high
12/4/2024	[Cisco Unified IP Phone Permissions, Privileges, and Access Controls (CVE-2007-1072)]	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

“Tue, 03 Dec 2024

ZDI-24-1642: Linux Kernel nftables Type Confusion Information Disclosure Vulnerability

- Link

—

” “Tue, 03 Dec 2024

ZDI-24-1641: Intel Computing Improvement Program PyInstaller Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 02 Dec 2024

ZDI-24-1640: XnSoft XnView Classic RWZ File Parsing Integer Underflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 02 Dec 2024

ZDI-24-1639: Hewlett Packard Enterprise Insight Remote Support processAtatchmentDataStream Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Mon, 02 Dec 2024

ZDI-24-1638: Hewlett Packard Enterprise Insight Remote Support validateAgainstXSD XML External Entity Processing Information Disclosure Vulnerability

- Link

—

” “Mon, 02 Dec 2024

ZDI-24-1637: Hewlett Packard Enterprise Insight Remote Support getDocumentRootElement XML External Entity Processing Information Disclosure Vulnerability

- Link

—

” “Mon, 02 Dec 2024

ZDI-24-1636: Hewlett Packard Enterprise Insight Remote Support DESTA Service Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Mon, 02 Dec 2024

ZDI-24-1635: Hewlett Packard Enterprise Insight Remote Support setInputStream XML External Entity Processing Information Disclosure Vulnerability

- Link

—

” “Mon, 02 Dec 2024

ZDI-24-1634: Hewlett Packard Enterprise AutoPass License Server XML External Entity Processing Information Disclosure Vulnerability

- Link

—

” “Mon, 02 Dec 2024

ZDI-24-1633: Hewlett Packard Enterprise AutoPass License Server SQL Injection Information Disclosure Vulnerability

- Link

—

” “Mon, 02 Dec 2024

ZDI-24-1632: Hewlett Packard Enterprise AutoPass License Server hsqldb Remote Code Execution

Vulnerability

- Link

—

” “Mon, 02 Dec 2024

ZDI-24-1631: Hewlett Packard Enterprise AutoPass License Server Authentication Bypass 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: (Dez)

Datum	Opfer	Land	Information
2024-12-02	Pembina Trails School Division	[CAN]	Link
2024-12-01	PIH Health	[USA]	Link

7 Ransomware-Erpressungen: (Dez)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-12-04	[islandphoto.com]	ransomhub	Link
2024-12-04	[troxlerlabs.com]	ransomhub	Link
2024-12-04	[hobokennj.gov]	threeam	Link
2024-12-04	[NTrust]	raworld	Link
2024-12-04	[copral.com.br]	lockbit3	Link
2024-12-04	[Deloitte UK]	BrainCipher	Link
2024-12-04	[uniaomarmores]	funksec	Link
2024-12-04	[hamptonsecurities.com]	blackbasta	Link
2024-12-04	[g-s.co.uk]	blackbasta	Link
2024-12-04	[cafezupas.com]	blackbasta	Link
2024-12-04	[westbankcorp.com]	blackbasta	Link
2024-12-04	[btci.com]	blackbasta	Link
2024-12-04	[beko-technologies.com]	blackbasta	Link
2024-12-04	[snatt.it]	blackbasta	Link
2024-12-04	[medicacorp.com]	blackbasta	Link
2024-12-04	[lornestewartgroup.com]	blackbasta	Link
2024-12-04	[vossko.de]	blackbasta	Link
2024-12-04	[www.certifiedinfosec.com]	apt73	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-12-04	[FF Steel]	sarcoma	Link
2024-12-03	[www.sefiso-atlantique.fr]	ransomhub	Link
2024-12-03	[marietta-city.org]	ransomhub	Link
2024-12-03	[westbornmarket.com]	ransomhub	Link
2024-12-04	[www.lasalle.com]	ransomhub	Link
2024-12-04	[kingdom]	funksec	Link
2024-12-04	[albazaar]	funksec	Link
2024-12-04	[rscn.org.jo]	funksec	Link
2024-12-04	[verificativa]	funksec	Link
2024-12-04	[intbizth]	funksec	Link
2024-12-04	[xui.one]	funksec	Link
2024-12-04	[x-cart automotive]	funksec	Link
2024-12-04	[IFA Paris]	funksec	Link
2024-12-04	[styched]	funksec	Link
2024-12-04	[Smart-it-partner]	funksec	Link
2024-12-04	[USA Network]	funksec	Link
2024-12-04	[Zero 5]	funksec	Link
2024-12-03	[Marine Stores Guide]	qilin	Link
2024-12-01	[internetway.com.br]	ransomhub	Link
2024-12-03	[www.iscinc93.com]	ransomhub	Link
2024-12-03	[www.fibrogen.com]	ransomhub	Link
2024-12-03	[www.z2data.com]	ransomhub	Link
2024-12-03	[www.giorgiovisconti.it]	ransomhub	Link
2024-12-03	[www.kiswire.com]	ransomhub	Link
2024-12-03	[www.dalgroup.com]	ransomhub	Link
2024-12-03	[www.goethe-university-frankfurt.de]	ransomhub	Link
2024-12-03	[www.wsgcpa.com]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-12-03	[www.siapenet.gov.br]	apt73	Link
2024-12-03	[InterCon Construction]	hunters	Link
2024-12-03	[Conteg]	hunters	Link
2024-12-03	[Royce Corporation]	BrainCipher	Link
2024-12-03	[ACM_IT]	argonauts	Link
2024-12-03	[RDC]	argonauts	Link
2024-12-03	[Goodwill North Central Texas]	rhysida	Link
2024-12-03	[Harel Insurance (Shirbit Server)]	handala	Link
2024-12-02	[New Age Micro]	lynx	Link
2024-12-02	[Billaud Segeba]	qilin	Link
2024-12-02	[salesgig.com]	darkvault	Link
2024-12-02	[KHKKLOW.com]	ransomhub	Link
2024-12-02	[G-ONE AUTO PARTS DE MÉXICO, S.A. DE C.V.]	BrainCipher	Link
2024-12-02	[Conlin’s Pharmacy (conlinspharmacy.com)]	fog	Link
2024-12-02	[Mmaynewagemicro]	lynx	Link
2024-12-02	[Avico Spice]	medusa	Link
2024-12-02	[Down East Granite]	medusa	Link
2024-12-02	[Wiley Metal Fabricating]	medusa	Link
2024-12-01	[shapesmfg.com]	ransomhub	Link
2024-12-01	[everde.com]	ransomhub	Link
2024-12-01	[qualitybillingservice.com]	ransomhub	Link
2024-12-01	[tascosaofficemachines.com]	ransomhub	Link
2024-12-01	[costelloeye.com]	ransomhub	Link
2024-12-01	[McKibbin]	incransom	Link
2024-12-01	[Alpine Ear Nose & Throat]	bianlian	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.