Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241107

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

HPE Aruba stopft Codeschmuggel-Lücken in Access Points

Firmware-Updates für HPE Aruba Access Points stopfen mehrere kritische Sicherheitslücken, die Angreifern das Einschleusen von Schadcode ermöglichen.

- Link

—

Synology korrigiert weitere kritische Pwn2Own-Sicherheitslücken

Synology-NAS waren ein beliebtes Ziel beim Pwn2Own-Wettbewerb in Irland. Der Hersteller stopft weitere, dort entdeckte kritische Sicherheitslücken.

- Link

—

Veritas Netbackup: Rechteausweitung in Windows möglich

Hersteller Veritas warnt vor einer Sicherheitslücke in Netbackup unter Windows. Angreifer können dadurch ihre Rechte ausweiten.

- Link

—

Android-Patchday: Updates stopfen zwei angegriffene Sicherheitslücken

Der Android-Patchday im November bringt Aktualisierungen mit, die unter anderem zwei bereits angegriffene Sicherheitslecks abdichten.

- Link

—

Zoho ManageEngine ADManager Plus: Angreifer können SQL-Befehle einschleusen

In ManageEngine ADManager Plus von Zohocorp können Angreifer eine SQL-Injection-Lücke missbrauchen und dadurch unbefugten Zugriff erlangen.

- Link

—

Okta: Sicherheitslücke in Verify gibt Angreifern Zugriff auf Passwörter

In Verify von Okta können Angreifer eine Sicherheitslücke im Windows-Agent missbrauchen, um Passwörter abzugreifen. Eine weitere Lücke betrifft Okta AD/LDAP.

- Link

—

Sicherheitsupdates: Schadcode-Attacken auf Synology-NAS möglich

Zwei während des Hackerwettbewerbs Pwn2Own entdeckte kritische Sicherheitslücken in NAS-Geräten von Synology wurden geschlossen.

- Link

—

Nvidia ConnectX, BlueField: Angreifer können Daten manipulieren

In aktuellen Firmwareversion hat Nvidia Sicherheitslücken im Netzwerkadapter ConnectX und der Computing-Plattform BlueField geschlossen.

- Link

—

Jetzt patchen! Ransomware-Attacken auf Server mit CyberPanel beobachtet

Angreifer nutzen kritische Schwachstellen in Servern aus, auf denen CyberPanel installiert ist. Eine abgesicherte Version ist verfügbar.

- Link

—

Qnap schließt NAS-Sicherheitslücken aus Hackerwettbewerb

NAS-Modelle von Qnap mit der Backupsoftware HBS 3 Hybrid Backup Sync sind angreifbar. Auch im SMB-Service wurde eine kritische Lücke geschlossen.

- 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	0.957580000	0.994990000	Link
CVE-2023-6895	0.925010000	0.990880000	Link
CVE-2023-6553	0.949860000	0.993740000	Link
CVE-2023-6019	0.932040000	0.991540000	Link
CVE-2023-6018	0.911590000	0.989860000	Link
CVE-2023-52251	0.947690000	0.993430000	Link
CVE-2023-4966	0.970850000	0.998240000	Link
CVE-2023-49103	0.947920000	0.993450000	Link
CVE-2023-48795	0.962520000	0.995820000	Link
CVE-2023-47246	0.962070000	0.995740000	Link
CVE-2023-46805	0.962030000	0.995730000	Link
CVE-2023-46747	0.972770000	0.998910000	Link
CVE-2023-46604	0.969640000	0.997780000	Link
CVE-2023-4542	0.941060000	0.992570000	Link
CVE-2023-43208	0.974790000	0.999780000	Link
CVE-2023-43177	0.957850000	0.995040000	Link
CVE-2023-42793	0.970830000	0.998240000	Link
CVE-2023-41892	0.905460000	0.989420000	Link
CVE-2023-41265	0.920970000	0.990510000	Link
CVE-2023-38205	0.955500000	0.994620000	Link
CVE-2023-38203	0.964750000	0.996350000	Link
CVE-2023-38146	0.920950000	0.990510000	Link
CVE-2023-38035	0.974570000	0.999680000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.967260000	0.997050000	Link
CVE-2023-3519	0.965540000	0.996590000	Link
CVE-2023-35082	0.963840000	0.996130000	Link
CVE-2023-35078	0.967840000	0.997230000	Link
CVE-2023-34993	0.973050000	0.999010000	Link
CVE-2023-34634	0.926130000	0.990980000	Link
CVE-2023-34362	0.969990000	0.997940000	Link
CVE-2023-34039	0.944770000	0.993050000	Link
CVE-2023-3368	0.928640000	0.991220000	Link
CVE-2023-33246	0.973040000	0.999010000	Link
CVE-2023-32315	0.973320000	0.999140000	Link
CVE-2023-30625	0.953680000	0.994320000	Link
CVE-2023-30013	0.962230000	0.995760000	Link
CVE-2023-29300	0.967820000	0.997230000	Link
CVE-2023-29298	0.968120000	0.997330000	Link
CVE-2023-28432	0.921730000	0.990590000	Link
CVE-2023-28343	0.962760000	0.995890000	Link
CVE-2023-28121	0.927310000	0.991090000	Link
CVE-2023-27524	0.970490000	0.998120000	Link
CVE-2023-27372	0.973760000	0.999340000	Link
CVE-2023-27350	0.969490000	0.997730000	Link
CVE-2023-26469	0.955890000	0.994680000	Link
CVE-2023-26360	0.963280000	0.996000000	Link
CVE-2023-26035	0.969120000	0.997620000	Link
CVE-2023-25717	0.950620000	0.993820000	Link
CVE-2023-25194	0.965880000	0.996690000	Link
CVE-2023-2479	0.961940000	0.995720000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-24489	0.972720000	0.998880000	Link
CVE-2023-23752	0.949040000	0.993610000	Link
CVE-2023-23397	0.902750000	0.989290000	Link
CVE-2023-23333	0.963480000	0.996050000	Link
CVE-2023-22527	0.970950000	0.998300000	Link
CVE-2023-22518	0.963120000	0.995970000	Link
CVE-2023-22515	0.973100000	0.999040000	Link
CVE-2023-21839	0.933960000	0.991770000	Link
CVE-2023-21554	0.955110000	0.994550000	Link
CVE-2023-20887	0.970370000	0.998060000	Link
CVE-2023-1698	0.916400000	0.990140000	Link
CVE-2023-1671	0.962340000	0.995800000	Link
CVE-2023-0669	0.971830000	0.998560000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 06 Nov 2024

[UPDATE] [hoch] bzip2: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit den Rechten des Dienstes

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in bzip2 ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen.

- Link

—

Wed, 06 Nov 2024

[UPDATE] [hoch] Red Hat OpenStack: Schwachstelle ermöglicht Erlangung erweiterter Privilegien

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat OpenStack ausnutzen, um erweiterte Privilegien zu erlangen.

- Link

—

Wed, 06 Nov 2024

[UPDATE] [hoch] Jenkins: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Jenkins ausnutzen, um beliebigen Code im Kontext des Dienstes auszuführen, Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.

- Link

—

Wed, 06 Nov 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im RADIUS Protokoll ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 06 Nov 2024

[UPDATE] [hoch] Django: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Django ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder vertrauliche Informationen offenzulegen.

- Link

—

Wed, 06 Nov 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, 06 Nov 2024

[UPDATE] [hoch] Jenkins: Mehrere Schwachstellen

Ein entfernter, authentisierter oder anonymer Angreifer kann mehrere Schwachstellen in Jenkins und verschiedenen Jenkins Plugins ausnutzen, um Informationen offenzulegen Sicherheitsvorkehrungen zu umgehen oder seine Rechte zu erweitern.

- Link

—

Wed, 06 Nov 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, Dateien zu manipulieren oder

beliebigen Code auszuführen.
- Link

—

Wed, 06 Nov 2024

[UPDATE] [hoch] Mozilla Firefox, ESR 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 oder einen Cross-Site-Scripting-Angriff durchzuführen.
- Link

—

Wed, 06 Nov 2024

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

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat Satellite ausnutzen, um Informationen offenzulegen und weitere, nicht spezifizierte Auswirkungen zu verursachen.
- Link

—

Wed, 06 Nov 2024

[UPDATE] [UNGEPATCHT] [kritisch] DrayTek Vigor: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter anonymer oder authentifizierter Angreifer kann mehrere Schwachstellen in DrayTek Vigor ausnutzen, um beliebigen Code auszuführen.
- Link

—

Wed, 06 Nov 2024

[NEU] [hoch] HCL BigFix WebUI: Mehrere Open Source Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in HCL BigFix WebU ausnutzen, um die Vertraulichkeit, Verfügbarkeit und Integrität zu gefährden.
- Link

—

Wed, 06 Nov 2024

[NEU] [hoch] Aruba ArubaOS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Aruba ArubaOS ausnutzen, um beliebige Betriebssystemkommandos auszuführen und um Zugriffsbeschränkungen zu umgehen.
- Link

—

Wed, 06 Nov 2024

[UPDATE] [hoch] Apple iOS und iPadOS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS

ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Wed, 06 Nov 2024

[NEU] [UNGEPATCHT] [hoch] D-LINK Router DIR-823G: Mehrere Schwachstellen ermöglichen Codeausführung

Ein Angreifer aus einem angrenzenden Netzwerk kann mehrere Schwachstellen im D-LINK Router DIR-823G ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 06 Nov 2024

[NEU] [hoch] Google Chrome: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen und potenziell um Code auszuführen.

- Link

—

Wed, 06 Nov 2024

[NEU] [hoch] Red Hat OpenShift: Schwachstelle ermöglicht Cross-Site Scripting

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat OpenShift ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen.

- Link

—

Tue, 05 Nov 2024

[NEU] [hoch] Red Hat Enterprise Linux (OpenEXR): Schwachstelle ermöglicht Manipulation von Dateien

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um Dateien zu manipulieren.

- Link

—

Tue, 05 Nov 2024

[NEU] [hoch] Microsoft NuGet: Schwachstelle ermöglicht Manipulation von Dateien

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Microsoft NuGet ausnutzen, um Dateien zu manipulieren.

- Link

—

Tue, 05 Nov 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen und einen Denial-of-Service-Zustand zu verursachen.
- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
11/6/2024	[RHEL 8 : krb5 (RHSA-2024:8794)]	critical
11/6/2024	[RHEL 9 : openexr (RHSA-2024:8801)]	critical
11/6/2024	[RHEL 8 : python-gevent (RHSA-2024:8834)]	critical
11/6/2024	[RHEL 8 : krb5 (RHSA-2024:8789)]	critical
11/6/2024	[Oracle Linux 8 : go-toolset:ol8 (ELSA-2024-8876)]	critical
11/6/2024	[AlmaLinux 8 : xmlrpc-c (ALSA-2024:8859)]	critical
11/6/2024	[AlmaLinux 8 : bzip2 (ALSA-2024:8922)]	critical
11/6/2024	[AlmaLinux 8 : python-gevent (ALSA-2024:8834)]	critical
11/6/2024	[AlmaLinux 8 : krb5 (ALSA-2024:8860)]	critical
11/6/2024	[RHEL 8 : go-toolset:rhel8 (RHSA-2024:8876)]	critical
11/6/2024	[Oracle Linux 8 : bzip2 (ELSA-2024-8922)]	critical
11/6/2024	[RHEL 8 : thunderbird (RHSA-2024:8790)]	high
11/6/2024	[RHEL 9 : Red Hat JBoss Enterprise Application Platform 8.0.4 Security update (Important) (RHSA-2024:8824)]	high
11/6/2024	[RHEL 8 : kernel (RHSA-2024:8856)]	high
11/6/2024	[RHEL 8 : haproxy (RHSA-2024:8874)]	high
11/6/2024	[RHEL 7 : xerces-c (RHSA-2024:8795)]	high
11/6/2024	[FreeBSD : chromium – multiple security fixes (ab254c9d-9c36-11ef-8c1c-a8a1599412c6)]	high

Datum	Schwachstelle	Bewertung
11/6/2024	[Oracle Linux 8 : python3.11 (ELSA-2024-8838)]	high
11/6/2024	[Oracle Linux 8 : python3.12 (ELSA-2024-8836)]	high
11/6/2024	[RHEL 9 : edk2 (RHSA-2024:8935)]	high
11/6/2024	[AlmaLinux 8 : haproxy (ALSA-2024:8849)]	high
11/6/2024	[AlmaLinux 8 : python3.12 (ALSA-2024:8836)]	high
11/6/2024	[AlmaLinux 8 : xorg-x11-server and xorg-x11-server-Xwayland (ALSA-2024:8798)]	high
11/6/2024	[AlmaLinux 8 : libtiff (ALSA-2024:8833)]	high
11/6/2024	[AlmaLinux 8 : kernel (ALSA-2024:8856)]	high
11/6/2024	[AlmaLinux 8 : python3.11 (ALSA-2024:8838)]	high
11/6/2024	[AlmaLinux 8 : kernel-rt (ALSA-2024:8870)]	high
11/6/2024	[GLSA-202411-03 : Ubiquiti UniFi: Privilege Escalation]	high
11/6/2024	[GLSA-202411-04 : EditorConfig core C library: arbitrary stack write]	high
11/6/2024	[Apache 2.4.x < 2.4.62 Multiple Vulnerabilities (Windows)]	high
11/6/2024	[RHEL 6 / 7 : rh-ror42-rubygem-actionpack (RHSA-2019:1149)]	high
11/6/2024	[RHEL 7 : ansible (RHSA-2019:0590)]	high
11/6/2024	[RHEL 7 : rh-nginx114-nginx (RHSA-2019:2775)]	high
11/6/2024	[Oracle Linux 9 : edk2 (ELSA-2024-8935)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Tue, 05 Nov 2024

ABB Cylon Aspect 3.08.00 Off-By-One

A vulnerability was identified in a ABB Cylon Aspect version 3.08.00 where an off-by-one error in array access could lead to undefined behavior and potential denial of service. The issue arises in a loop that iterates over an array using a less than or equals to condition, allowing access to an out-of-bounds

index. This can trigger errors or unexpected behavior when processing data, potentially crashing the application. Successful exploitation of this vulnerability can lead to a crash or disruption of service, especially if the script handles large data sets.

- Link

—

” “Mon, 04 Nov 2024

Sysax Multi Server 6.99 SSH Denial Of Service

Sysax Multi Server version 6.9.9 suffers from an SSH related denial of service vulnerability.

- Link

—

” “Mon, 04 Nov 2024

Sysax Multi Server 6.99 Cross Site Scripting

Sysax Multi Server version 6.9.9 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 04 Nov 2024

IBM Security Verify Access 32 Vulnerabilities

IBM Security Verify Access versions prior to 10.0.8 suffer from authentication bypass, reuse of private keys, local privilege escalation, weak settings, outdated libraries, missing password, hardcoded secrets, remote code execution, missing authentication, null pointer dereference, and lack of privilege separation vulnerabilities.

- Link

—

” “Mon, 04 Nov 2024

IBM Security Verify Access Appliance Insecure Transit / Hardcoded Passwords

IBM Security Verify Access Appliance suffers from multiple insecure transit vulnerabilities, hardcoded passwords, and uninitialized variables. ibmsecurity versions prior to 2024.4.5 are affected.

- Link

—

” “Mon, 04 Nov 2024

ESET NOD32 Antivirus 18.0.12.0 Unquoted Service Path

ESET NOD32 Antivirus version 18.0.12.0 suffers from an unquoted service path vulnerability.

- Link

—

” “Mon, 04 Nov 2024

SQLite3 generate_series Stack Buffer Underflow

SQLite3 suffers from a stack buffer underflow condition in seriesBestIndex in the generate_series extension.

- Link

—

” “Mon, 04 Nov 2024

Linux khugepaged Race Conditions

khugepaged in Linux races with rmap-based zap, races with GUP-fast, and fails to call MMU notifiers.

- Link

—

” “Fri, 01 Nov 2024

Ping Identity PingIDM 7.5.0 Query Filter Injection

Ping Identity PingIDM versions 7.0.0 through 7.5.0 enabled an attacker with read access to the User collection, to abuse API query filters in order to obtain managed and/or internal user’s passwords in either plaintext or encrypted variants, based on configuration. The API clearly prevents the password in either plaintext or encrypted to be retrieved by any other means, as this field is set as protected under the User object. However, by injecting a malicious query filter, using password as the field to be filtered, an attacker can perform a blind brute-force on any victim’s user password details (encrypted object or plaintext string).

- Link

—

” “Fri, 01 Nov 2024

ABB Cylon Aspect 3.08.01 File Upload MD5 Checksum Bypass

ABB Cylon Aspect version 3.08.01 has a vulnerability in caldavInstall.php, caldavInstallAgendav.php, and caldavUpload.php files, where the presence of an EXPERTMODE parameter activates a badassMode feature. This mode allows an unauthenticated attacker to bypass MD5 checksum validation during file uploads. By enabling badassMode and setting the skipChecksum parameter, the system skips integrity verification, allowing attackers to upload or install altered CalDAV zip files without authentication. This vulnerability permits unauthorized file modifications, potentially exposing the system to tampering or malicious uploads.

- Link

—

” “Fri, 01 Nov 2024

Packet Storm New Exploits For October, 2024

This archive contains all of the 128 exploits added to Packet Storm in October, 2024.

- Link

—

” “Fri, 01 Nov 2024

SmartAgent 1.1.0 Remote Code Execution

SmartAgent version 1.1.0 suffers from an unauthenticated remote code execution vulnerability in youtubeInfo.php.

- Link

—

” “Fri, 01 Nov 2024

SmartAgent 1.1.0 Server-Side Request Forgery

SmartAgent version 1.1.0 suffers from a server-side request forgery vulnerability.

- Link

—

” “Fri, 01 Nov 2024

SmartAgent 1.1.0 SQL Injection

SmartAgent version 1.1.0 suffers from multiple unauthenticated remote SQL injection vulnerabilities.

- Link

—

” “Thu, 31 Oct 2024

WordPress Automatic 3.92.0 Path Traversal / Server-Side Request Forgery

WordPress Automatic plugin versions 3.92.0 and below proof of concept exploit that demonstrates path traversal and server-side request forgery vulnerabilities.

- Link

—

” “Thu, 31 Oct 2024

Qualitor 8.24 Server-Side Request Forgery

Qualitor versions 8.24 and below suffer from an unauthenticated server-side request forgery vulnerability.

- Link

—

” “Thu, 31 Oct 2024

CyberPanel Command Injection

Proof of concept exploit for a command injection vulnerability in CyberPanel. This vulnerability enables unauthenticated attackers to inject and execute arbitrary commands on vulnerable servers by sending crafted OPTIONS HTTP requests to /dns/getresetstatus and /ftp/getresetstatus endpoints, potentially leading to full system compromise. Versions prior to 1c0c6cb appear to be affected.

- Link

—

” “Thu, 31 Oct 2024

Skyhigh Client Proxy Policy Bypass

Proof of concept code for a flaw where a malicious insider can bypass the existing policy of Skyhigh Client Proxy without a valid release code.

- Link

—

” “Wed, 30 Oct 2024

WordPress WP-Automatic SQL Injection

This Metasploit module exploits an unauthenticated SQL injection vulnerability in the WordPress wp-automatic plugin versions prior to 3.92.1 to achieve remote code execution. The vulnerability allows the attacker to inject and execute arbitrary SQL commands, which can be used to create a malicious administrator account. The password for the new account is hashed using MD5. Once the administrator account is created, the attacker can upload and execute a malicious plugin, leading to full control over the WordPress site.

- Link

—

” “Wed, 30 Oct 2024

ABB Cylon Aspect 3.08.01 jsonProxy.php Username Enumeration

ABB Cylon Aspect version 3.08.01 is vulnerable to username enumeration in the jsonProxy.php endpoint. An unauthenticated attacker can interact with the UserManager servlet to enumerate valid usernames on the system. Since jsonProxy.php proxies requests to internal services without requiring authentication, attackers can gain unauthorized insights into valid usernames.

- Link

—

” “Wed, 30 Oct 2024

ABB Cylon Aspect 3.08.01 jsonProxy.php Information Disclosure

ABB Cylon Aspect version 3.08.01 is vulnerable to unauthorized information disclosure in the jsonProxy.php endpoint. An unauthenticated attacker can retrieve sensitive system information, including system time, uptime, memory usage, and network load statistics. The jsonProxy.php endpoint proxies these requests to internal services without requiring authentication, allowing attackers to obtain detailed system status data, which could aid in further attacks by revealing operational characteristics and resource utilization.

- Link

—

” “Wed, 30 Oct 2024

ABB Cylon Aspect 3.08.01 jsonProxy.php Unauthenticated Remote SSH Service Control

ABB Cylon Aspect version 3.08.01 is vulnerable to unauthorized SSH service configuration changes via the jsonProxy.php endpoint. An unauthenticated attacker can enable or disable the SSH service on the server by accessing the FTControlServlet with the sshenable parameter. The jsonProxy.php script proxies requests to localhost without enforcing authentication, allowing attackers to modify SSH settings and potentially gain further unauthorized access to the system.

- Link

—

” “Wed, 30 Oct 2024

ABB Cylon Aspect 3.08.01 jsonProxy.php Denial Of Service

ABB Cylon Aspect version 3.08.01 is vulnerable to an unauthenticated denial of service attack in the jsonProxy.php endpoint. An attacker can remotely restart the main Java server by accessing the FTControlServlet with the restart parameter. The endpoint proxies requests to localhost without requiring authentication, enabling attackers to disrupt system availability by repeatedly triggering server restarts.

- Link

—

” “Wed, 30 Oct 2024

ABB Cylon Aspect 3.08.01 jsonProxy.php Unauthenticated Project Download

ABB Cylon Aspect version 3.08.01 is vulnerable to an unauthorized project file disclosure in jsonProxy.php. An unauthenticated remote attacker can issue a GET request abusing the DownloadProject servlet to download sensitive project files. The jsonProxy.php script bypasses authentication by proxying requests to localhost (AspectFT Automation Application Server), granting remote attackers unauthorized access to internal Java servlets. This exposes potentially sensitive project data and configuration details without requiring authentication.

- Link

—

” “Wed, 30 Oct 2024

ABB Cylon Aspect 3.08.01 jsonProxy.php Servlet Inclusion Authentication Bypass

ABB Cylon Aspect version 3.08.01 is vulnerable to remote, arbitrary servlet inclusion. The jsonProxy.php endpoint allows unauthenticated remote attackers to access internal services by proxying requests to localhost. This results in an authentication bypass, enabling attackers to interact with multiple java servlets without authorization, potentially exposing sensitive system functions and information.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Wed, 06 Nov 2024

ZDI-24-1460: Centreon updateContactHostCommands_MC SQL Injection Privilege Escalation Vulnerability

- Link

—

” “Wed, 06 Nov 2024

ZDI-24-1459: Centreon updateAccessGroupLinks_MC SQL Injection Privilege Escalation Vulnerabi-

lity

- Link

—

” “Wed, 06 Nov 2024

ZDI-24-1458: Centreon updateContactServiceCommands_MC SQL Injection Privilege Escalation Vulnerability

- Link

—

” “Wed, 06 Nov 2024

ZDI-24-1457: Delta Electronics InfraSuite Device Master _gExtraInfo Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Tue, 05 Nov 2024

ZDI-24-1456: Linux Kernel ksmbd Session Race Condition Remote Code Execution Vulnerability

- Link

—

” “Tue, 05 Nov 2024

ZDI-24-1455: Linux Kernel Net Scheduler ATM Queuing Discipline Use-After-Free Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 05 Nov 2024

ZDI-24-1454: Linux Kernel nftables Improper Validation of Array Index Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 05 Nov 2024

ZDI-24-1453: X.Org Server XkbSetCompatMap Heap-based Buffer Overflow Privilege Escalation Vulnerability

- Link

—

” “Mon, 04 Nov 2024

ZDI-24-1452: Autodesk AutoCAD CATPART File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

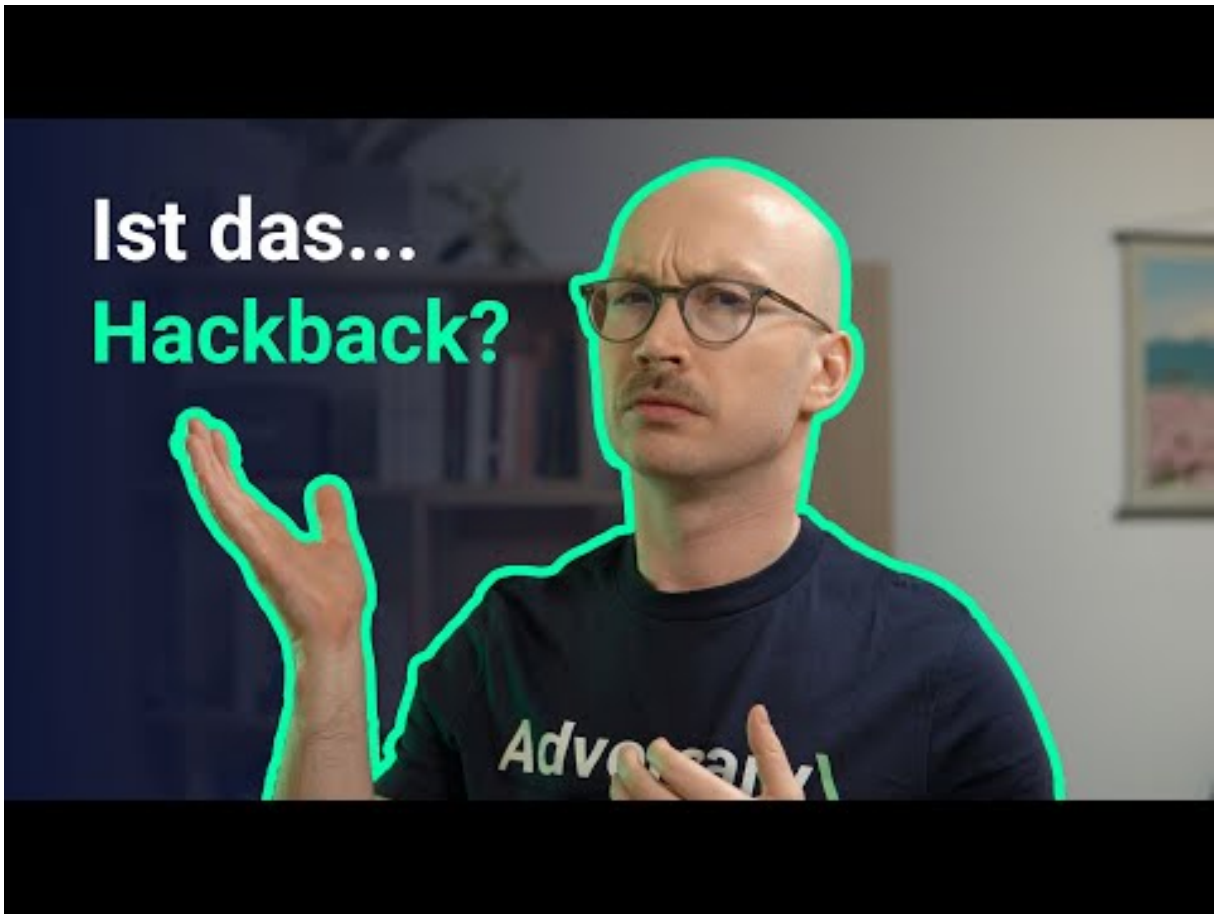
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Sophos spielt die UNO Reverse Karte (+ Redline Stealer)



Zum Youtube Video

6 Cyberangriffe: (Nov)

Datum	Opfer	Land	Information
2024-11-05	Lojas Marisa	[BRA]	Link
2024-11-04	Avis de Torino	[ITA]	Link
2024-11-02	Memorial Hospital and Manor	[USA]	Link
2024-11-02	Kumla kommun	[SWE]	Link
2024-11-01	South East Technological University (SETU)	[IRL]	Link

7 Ransomware-Erpressungen: (Nov)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-11-06	[www.msdl.ca]	ransomhub	Link
2024-11-07	[Postcard Mania]	play	Link
2024-11-07	[New Law]	hunters	Link
2024-11-06	[klinkamkurpark]	helldown	Link
2024-11-06	[hausdesstiftens.org]	helldown	Link
2024-11-06	[nightnurse.ch]	helldown	Link
2024-11-06	[fuelco]	helldown	Link
2024-11-06	[VALLEYFIRM]	helldown	Link
2024-11-06	[children]	helldown	Link
2024-11-06	[knoxlawcenter]	helldown	Link
2024-11-06	[AMERICANVENTURE]	helldown	Link
2024-11-06	[CSIKBS]	helldown	Link
2024-11-06	[SANJACINTOCOUNY]	helldown	Link
2024-11-06	[compassfs]	helldown	Link
2024-11-06	[lacliniqueducoureur]	helldown	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-11-06	[TIVOLI-33]	helldown	Link
2024-11-06	[qualiform.cz]	helldown	Link
2024-11-06	[SMARTS-ENGINEER]	helldown	Link
2024-11-06	[brandenburgerplumbing.com]	ransomhub	Link
2024-11-06	[arcoexc.com]	ransomhub	Link
2024-11-06	[Lincoln University]	meow	Link
2024-11-06	[Cape Cod Regional Technical High School (capetech.us)]	fog	Link
2024-11-06	[GSR Andrade Architects (gsr-andrade.com)]	fog	Link
2024-11-05	[metroelectric.com]	ransomhub	Link
2024-11-05	[sector5.ro]	ransomhub	Link
2024-11-05	[Paragon Plastics]	play	Link
2024-11-05	[Delfin Design & Manufacturing]	play	Link
2024-11-05	[Smitty’s Supply]	play	Link
2024-11-05	[S & W Kitchens]	play	Link
2024-11-05	[Dome Construction]	play	Link
2024-11-06	[Interoute agency]	lynx	Link
2024-11-06	[LmayInteroute agency]	lynx	Link
2024-11-05	[pacificglazing.com]	ransomhub	Link
2024-11-05	[nwhealthporter.com]	ransomhub	Link
2024-11-05	[wexfordcounty.org]	embargo	Link
2024-11-05	[ebrso]	qilin	Link
2024-11-05	[Model Die & Mold]	lynx	Link
2024-11-04	[mh-m.org]	embargo	Link
2024-11-05	[Falco Sult]	bianlian	Link
2024-11-05	[apoyoconsultoria.com]	ransomhub	Link
2024-11-05	[Webb Institute]	incransom	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-11-05	[Fylde Coast Academy Trust]	rhysida	Link
2024-11-04	[sundt.com]	ransomhub	Link
2024-11-04	[Memorial Hospital & Manor]	embargo	Link
2024-11-02	[Scolari]	dragonforce	Link
2024-11-05	[McMillan Electric Company]	medusa	Link
2024-11-04	[maxdata.com.br]	ransomhub	Link
2024-11-04	[goodline.com.au]	ransomhub	Link
2024-11-04	[kenanasugarcompany.com]	ransomhub	Link
2024-11-04	[www.schweiker.de]	ransomhub	Link
2024-11-04	[www.drbutlerandassociates.com]	ransomhub	Link
2024-11-04	[www.mssupply.com]	ransomhub	Link
2024-11-04	[fullfordelectric.com]	ransomhub	Link
2024-11-04	[College of Business - Tanzania]	hellcat	Link
2024-11-04	[Ministry of Education - Jordan]	hellcat	Link
2024-11-04	[Schneider Electric - France]	hellcat	Link
2024-11-04	[International University of Sarajevo]	medusa	Link
2024-11-04	[Whitaker Construction Group]	medusa	Link
2024-11-04	[European External Action Service (EEAS)]	hunters	Link
2024-11-04	[csucontracting.com]	ransomhub	Link
2024-11-04	[redphoenixconstruction.com]	ransomhub	Link
2024-11-04	[Air Specialists Heating & Air Conditioning]	hunters	Link
2024-11-03	[krigerconstruction.com]	ransomhub	Link
2024-11-03	[caseconstruction.com]	ransomhub	Link
2024-11-03	[lambertstonecommercial.com]	ransomhub	Link
2024-11-04	[Doctor 24x7]	killsec	Link
2024-11-03	[Hemubo]	hunters	Link
2024-11-03	[Elad municipality]	handala	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-11-03	[Russell Law Firm, LLC]	bianlian	Link
2024-11-03	[L & B Transport, L.L.C.]	bianlian	Link
2024-11-03	[guardianhc]	stormous	Link
2024-11-02	[bravodigitaltrader.co.uk]	ransomhub	Link
2024-11-02	[SVP Worldwide]	blacksuit	Link
2024-11-02	[Sumitomo]	killsec	Link
2024-11-01	[DieTech North America]	qilin	Link
2024-11-01	[www.fatboysfleetandauto.com]	ransomhub	Link
2024-11-01	[www.tigre.gob.ar]	ransomhub	Link
2024-11-01	[www.usm.cl]	ransomhub	Link
2024-11-01	[lighthouseelectric.com]	ransomhub	Link
2024-11-01	[JS McCarthy Printers]	play	Link
2024-11-01	[CGR Technologies]	play	Link
2024-11-01	[lumiplan.com]	cactus	Link
2024-11-01	[United Sleep Diagnostics]	medusa	Link
2024-11-01	[eap.gr]	ransomhub	Link
2024-11-01	[vikurverk.is]	lockbit3	Link
2024-11-01	[mirandaproduce.com.ve]	lockbit3	Link
2024-11-01	[Cerp Bretagne Nord]	hunters	Link
2024-11-01	[Hope Valley Recovery]	rhysida	Link
2024-11-01	[lsst.ac]	cactus	Link
2024-11-01	[MCNA Dental]	everest	Link
2024-11-01	[Arctrade]	everest	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.