
Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241103



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	22
5.0.1 AI Girlfriends HACKED (Da steht uns noch was bevor)	22
6 Cyberangriffe: (Nov)	23
7 Ransomware-Erpressungen: (Nov)	23
8 Quellen	24
8.1 Quellenverzeichnis	24
9 Impressum	25

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

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](#)

—

Google Chrome: Kritische Sicherheitslücke gestopft

Das wöchentliche Update für Googles Chrome-Webbrowser schließt dieses Mal eine als kritisches Risiko eingestufte Sicherheitslücke.

- [Link](#)

—

Sicherheitsupdates: Firefox und Thunderbird gegen Schadcode-Attacken gerüstet

Angreifer können die Browser Firefox und Firefox ESR und den Mailclient Thunderbird unter anderem abstürzen lassen.

- [Link](#)

—

IBM App Connect Enterprise: Angreifer können Anmeldung umgehen

Die Entwickler von IBM haben zwei Sicherheitslücken in App Connect Enterprise Certified Container geschlossen. Attacken sind aber nicht ohne Weiteres möglich.

- [Link](#)

VMware Tanzu Spring Security: Umgehung von Autorisierungsregeln möglich

In VMware Tanzu Spring Security klafft eine kritische Sicherheitslücke, die Angreifern die Umgehung von Autorisierungsregeln ermöglicht.

- [Link](#)

Nvidia: Rechteauserweiterung durch Sicherheitslücken in Grafiktreibern möglich

Nvidia warnt vor mehreren Sicherheitslücken in den Grafiktreibern, die etwa das Ausweiten der Rechte ermöglichen. Updates stehen bereit.

- [Link](#)

Cisco meldet mehr als 35 Sicherheitslücken in Firewall-Produkten

Ciscos ASA, Firepower und Secure Firewall Management Center weisen teils kritische Sicherheitslücken auf. Mehr als 35 schließen nun verfügbare Updates.

- [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	0.994980000	Link
CVE-2023-6895	0.925010000	0.990830000	Link
CVE-2023-6553	0.945310000	0.993070000	Link
CVE-2023-6019	0.932040000	0.991520000	Link
CVE-2023-6018	0.911590000	0.989780000	Link
CVE-2023-52251	0.947690000	0.993410000	Link
CVE-2023-4966	0.970850000	0.998230000	Link
CVE-2023-49103	0.947920000	0.993430000	Link
CVE-2023-48795	0.962520000	0.995810000	Link
CVE-2023-47246	0.960640000	0.995480000	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	0.992550000	Link
CVE-2023-43208	0.974790000	0.999790000	Link
CVE-2023-43177	0.957850000	0.995020000	Link
CVE-2023-42793	0.970830000	0.998230000	Link
CVE-2023-41892	0.905460000	0.989330000	Link
CVE-2023-41265	0.920970000	0.990450000	Link
CVE-2023-38205	0.955500000	0.994620000	Link
CVE-2023-38203	0.964750000	0.996330000	Link
CVE-2023-38146	0.920950000	0.990450000	Link
CVE-2023-38035	0.974570000	0.999680000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.967260000	0.997040000	Link
CVE-2023-3519	0.965540000	0.996580000	Link
CVE-2023-35082	0.965310000	0.996530000	Link
CVE-2023-35078	0.967840000	0.997230000	Link
CVE-2023-34993	0.973050000	0.999020000	Link
CVE-2023-34634	0.923140000	0.990640000	Link
CVE-2023-34362	0.969990000	0.997940000	Link
CVE-2023-34039	0.944770000	0.993010000	Link
CVE-2023-3368	0.928640000	0.991160000	Link
CVE-2023-33246	0.971590000	0.998480000	Link
CVE-2023-32315	0.973480000	0.999180000	Link
CVE-2023-30625	0.953680000	0.994320000	Link
CVE-2023-30013	0.962230000	0.995750000	Link
CVE-2023-29300	0.967820000	0.997220000	Link
CVE-2023-29298	0.968120000	0.997330000	Link
CVE-2023-28432	0.921730000	0.990530000	Link
CVE-2023-28343	0.962760000	0.995880000	Link
CVE-2023-28121	0.927310000	0.991030000	Link
CVE-2023-27524	0.970490000	0.998110000	Link
CVE-2023-27372	0.973760000	0.999330000	Link
CVE-2023-27350	0.969490000	0.997730000	Link
CVE-2023-26469	0.955890000	0.994690000	Link
CVE-2023-26360	0.963280000	0.995990000	Link
CVE-2023-26035	0.969120000	0.997610000	Link
CVE-2023-25717	0.950620000	0.993800000	Link
CVE-2023-25194	0.965880000	0.996680000	Link
CVE-2023-2479	0.961940000	0.995710000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-24489	0.972720000	0.998880000	Link
CVE-2023-23752	0.949000000	0.993570000	Link
CVE-2023-23397	0.902750000	0.989210000	Link
CVE-2023-23333	0.963480000	0.996040000	Link
CVE-2023-22527	0.970950000	0.998290000	Link
CVE-2023-22518	0.965000000	0.996400000	Link
CVE-2023-22515	0.973250000	0.999110000	Link
CVE-2023-21839	0.941470000	0.992590000	Link
CVE-2023-21554	0.955110000	0.994550000	Link
CVE-2023-20887	0.971130000	0.998340000	Link
CVE-2023-1698	0.916400000	0.990080000	Link
CVE-2023-1671	0.962340000	0.995790000	Link
CVE-2023-0669	0.971830000	0.998550000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 01 Nov 2024

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

Ein Angreifer kann eine Schwachstelle in OpenSSL ausnutzen, um einen Denial of Service Angriff durchzuführen oder unbekannte Auswirkungen zu verursachen.

- [Link](#)

—

Fri, 01 Nov 2024

[UPDATE] [hoch] GNU Emacs: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in GNU Emacs ausnutzen, um beliebigen Programmcode auszuführen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Fri, 01 Nov 2024

[UPDATE] [hoch] GNU libc: Schwachstelle ermöglicht Codeausführung

Ein Angreifer kann eine Schwachstelle in GNU libc ausnutzen, um einen Denial-of-Service-Zustand zu verursachen, Code auszuführen oder seine Privilegien zu erweitern.

- [Link](#)

—

Fri, 01 Nov 2024

[UPDATE] [hoch] GNU Emacs: Schwachstelle ermöglicht Codeausführung

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

- [Link](#)

—

Fri, 01 Nov 2024

[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, 01 Nov 2024

[UPDATE] [hoch] Apache Camel und mehrere Red Hat Produkte: Mehrere Schwachstellen

Ein entfernter anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Apache Camel und in mehreren Red Hat-Produkten ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen preiszugeben und beliebigen Code auszuführen.

- [Link](#)

—

Fri, 01 Nov 2024

[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, 01 Nov 2024

[NEU] [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](#)

—

Fri, 01 Nov 2024

[NEU] [hoch] Rockwell Automation FactoryTalk ThinManager: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Rockwell Automation FactoryTalk ThinManager ausnutzen, um Dateien zu manipulieren oder einen Denial of Service zu verursachen.

- [Link](#)

—

Fri, 01 Nov 2024

[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen, seine Adresse zu spoofen, Informationen offenzulegen oder einen Denial of Service zu verursachen.

- [Link](#)

—

Fri, 01 Nov 2024

[UPDATE] [hoch] Eclipse Jetty: Mehrere Schwachstellen ermöglichen Denial of Service

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Eclipse Jetty ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Fri, 01 Nov 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service zu verursachen.

- [Link](#)

—

Fri, 01 Nov 2024

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

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in verschiedenen Komponenten von Red Hat Enterprise Linux ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand auszulösen.

- [Link](#)

—

Fri, 01 Nov 2024

[UPDATE] [hoch] Xerox FreeFlow Print Server: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Xerox FreeFlow Print Server ausnutzen, um die Vertraulichkeit, Verfügbarkeit und Integrität des Systems zu gefährden

- [Link](#)

—

Fri, 01 Nov 2024

[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Fri, 01 Nov 2024

[UPDATE] [hoch] QT: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonymmer Angreifer kann eine Schwachstelle in QT ausnutzen, um Informationen offenzulegen.

- [Link](#)

—

Fri, 01 Nov 2024

[UPDATE] [hoch] Node.js: Mehrere Schwachstellen

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Code auszuführen oder um Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

—

Fri, 01 Nov 2024

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

Ein entfernter anonymmer 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, 01 Nov 2024

[UPDATE] [hoch] CUPS: Mehrere Schwachstellen ermöglichen Ausführung von beliebigem Programmcode

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in CUPS ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen und um Informationen offenzulegen.

- [Link](#)

—

Fri, 01 Nov 2024

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

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Thunderbird ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmaßnahmen zu umgehen, Daten zu manipulieren, einen Denial-of-Service-Zustand zu erzeugen und vertrauliche

Informationen preiszugeben.

- [Link](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
11/2/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : python-waitress (SUSE-SU-2024:3876-1)]	critical
11/2/2024	[Oracle Linux 9 : firefox (ELSA-2024-8726)]	high
11/2/2024	[Oracle Linux 8 : firefox (ELSA-2024-8729)]	high
11/2/2024	[Fedora 40 : mysql8.0 (2024-0c1c9227e5)]	high
11/2/2024	[SUSE SLES15 Security Update : openssl-3 (SUSE-SU-2024:3871-1)]	high
11/2/2024	[SUSE SLES15 Security Update : xorg-x11-server (SUSE-SU-2024:3866-1)]	high
11/2/2024	[SUSE SLED15 / SLES15 Security Update : xorg-x11-server (SUSE-SU-2024:3867-1)]	high
11/2/2024	[SUSE SLED15 / SLES15 Security Update : ruby2.5 (SUSE-SU-2024:3874-1)]	high
11/2/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : cups-filters (SUSE-SU-2024:3863-1)]	high
11/2/2024	[SUSE SLES15 Security Update : webkit2gtk3 (SUSE-SU-2024:3870-1)]	high
11/2/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : rubygem-bundler (SUSE-SU-2024:3873-1)]	high
11/2/2024	[SUSE SLES15 Security Update : openssl-1_1 (SUSE-SU-2024:3872-1)]	high

Datum	Schwachstelle	Bewertung
11/2/2024	[SUSE SLES15 Security Update : rubygem-actionpack-5_1 (SUSE-SU-2024:3877-1)]	high
11/2/2024	[SUSE SLED15 / SLES15 Security Update : webkit2gtk3 (SUSE-SU-2024:3869-1)]	high
11/2/2024	[FreeBSD : chromium – multiple security fixes (e17384ef-c5e8-4b5d-bb62-c13405e7f1f7)]	high
11/2/2024	[CBL Mariner 2.0 Security Update: php (CVE-2024-8927)]	high
11/2/2024	[CBL Mariner 2.0 Security Update: php (CVE-2024-8926)]	high
11/1/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.10-2024-072)]	high
11/1/2024	[Amazon Linux 2 : python-pip (ALAS-2024-2679)]	high
11/1/2024	[Amazon Linux 2 : libgsf (ALAS-2024-2681)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“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 badass-Mode 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](#)

—

” “Wed, 30 Oct 2024

ABB Cylon Aspect 3.08.01 jsonProxy.php Unauthenticated Credential Disclosure

ABB Cylon Aspect version 3.08.01 allows an unauthenticated attacker to disclose credentials in plain-text.

- [Link](#)

—

” “Wed, 30 Oct 2024

ABB Cylon Aspect 3.08.01 jsonProxy.php Cross Site Scripting

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated reflected cross-site scripting vulnerability. Input passed to the GET parameters query and application is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML/JS code in a user's browser session in context of an affected site.

- [Link](#)

—

” “Tue, 29 Oct 2024

Xerox Printers Authenticated Remote Code Execution

Various Xerox printers, such as models EC80xx, AltaLink, VersaLink, and WorkCentre, suffer from an authenticated remote code execution vulnerability.

- [Link](#)

—

” “Tue, 29 Oct 2024

ABB Cylon Aspect 3.08.01 Active Debug Data Exposure

ABB Cylon Aspect version 3.08.01 is deployed to unauthorized actors with debugging code still enabled or active, which can create unintended entry points or expose sensitive information.

- [Link](#)

—

” “Tue, 29 Oct 2024

Booked Scheduler 2.8.5 Cross Site Scripting / Open Redirection

Booked Scheduler version 2.8.5 suffers from cross site scripting and open redirection vulnerabilities.

- [Link](#)

—

” “Tue, 29 Oct 2024

UP-RESULT PRO 1.0 SQL Injection

UP-RESULT PRO version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 28 Oct 2024

ABB Cylon Aspect 3.08.01 getApplicationNamesJS.php Building/Project Name Exposure

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated building/project name exposure vulnerability.

- [Link](#)

—

” “Fri, 25 Oct 2024

Lawo AG vsm LTC Time Sync Path Traversal

Lawo AG vsm LTC Time Sync versions prior to 4.5.6.0 suffer from a path traversal vulnerability.

- [Link](#)

—

”

4.2 0-Days der letzten 5 Tage

“Thu, 31 Oct 2024

ZDI-24-1451: Apple macOS ICC Profile Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1450: Apple macOS ICC Profile Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1449: Apple macOS CoreFoundation Font Glyphs Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1448: Apple macOS ICC Profile Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1447: Apple macOS ICC Profile Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1446: Apple macOS ICC Profile Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1445: Apple macOS ICC Profile Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1444: Apple SceneKit Improper Validation of Array Index Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1443: Apple macOS ImageIO JP2 Image Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1442: Apple macOS CoreText Font Ligature Caret List Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1441: Autodesk AutoCAD SLDPRT File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1440: Autodesk AutoCAD SLDPRT File Parsing Memory Corruption Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1439: Autodesk AutoCAD SLDPRT File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1438: Autodesk AutoCAD MODEL File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1437: Autodesk AutoCAD SLDPRT File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1436: Autodesk AutoCAD 3DM File Parsing Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1435: Autodesk AutoCAD 3DM File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1434: Autodesk AutoCAD CATPART File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1433: Autodesk AutoCAD MODEL File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1432: Autodesk AutoCAD MODEL File Parsing Use-After-Free Remote Code Execution Vul-

nerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1431: Autodesk AutoCAD STEP File Parsing Memory Corruption Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1430: Autodesk AutoCAD ATranslators STEP File Parsing Memory Corruption Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1429: Autodesk AutoCAD ATranslators STP File Parsing Memory Corruption Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1428: Autodesk AutoCAD ATranslators 3DM File Parsing Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1427: Autodesk AutoCAD ATranslators CATPART File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1426: Autodesk AutoCAD DXF File Parsing Uninitialized Variable Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1425: Autodesk AutoCAD DWG File Parsing Memory Corruption Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1424: Autodesk AutoCAD DWG File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 31 Oct 2024

ZDI-24-1423: Autodesk AutoCAD DWG File Parsing Memory Corruption Remote Code Execution Vulnerability

- [Link](#)

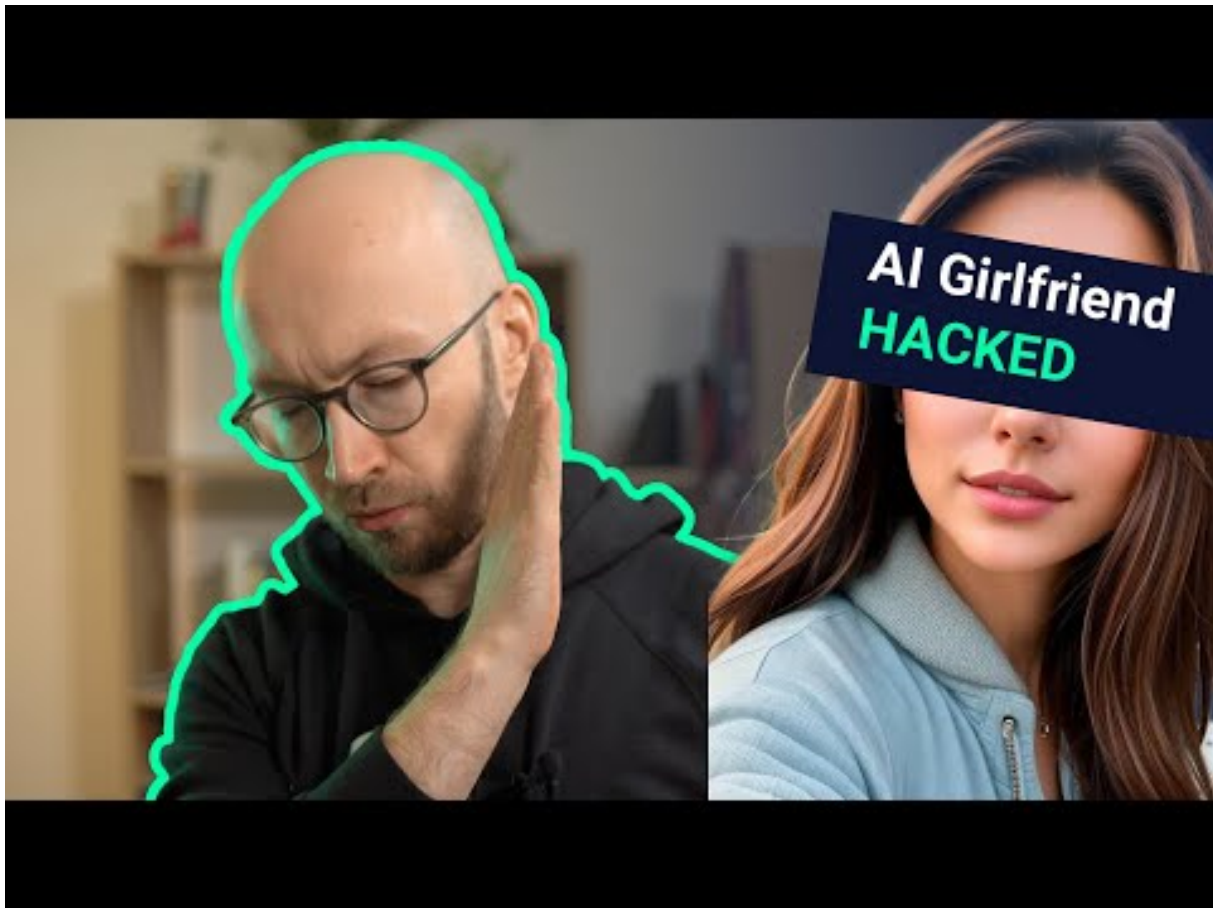
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 AI Girlfriends HACKED (Da steht uns noch was bevor)



[Zum Youtube Video](#)

6 Cyberangriffe: (Nov)

Datum	Opfer	Land	Information
2024-11-01	South East Technological University (SETU)	[IRL]	Link

7 Ransomware-Erpressungen: (Nov)

Datum	Opfer	Ransomware-Gruppe	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	[Imprimerie Peau]	qilin	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

Datum	Opfer	Ransomware-Gruppe	Webseite
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.