Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241011

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

Kritische Fortinet-Sicherheitslücke wird angegriffen
Die US-amerikanische IT-Sicherheitsbehörde CISA warnt, dass eine ältere Lücke in Fortinet-Produkten aktuell angegriffen wird.
- Link

—

Firefox-Notfall-Update stopft angegriffenes Sicherheitsleck
Neue Versionen von Firefox schließen Sicherheitslücken, die bereits in freier Wildbahn angegriffen werden.
- Link

—

HP Business-Notebooks: Hotkey-Unterstützung ermöglicht Rechteausweitung
Hewlett Packard warnt vor einer Schwachstelle im Hotkey-Support von Business-Notebooks. Angreifer können dadurch ihre Rechte ausweiten.
- Link

—

Wordpress-Plug-in: Abermals gravierende Sicherheitslücke in Litespeed Cache
Auf mehr als sechs Millionen Websites lauert eine schwerwiegende Schwachstelle im Wordpress-Plug-in Litespeed Cache. Ein Update steht bereit.
- Link

—

Ivanti stopft ausgenutzte Sicherheitslücken und mehr
Ivanti aktualisiert mehrere Software-Pakete. Darunter CSA, die bereits attackiert wird, oder Connect Secure mit kritischen Lecks.
- Link

—

Adobe-Patchday: Neun Produkte mit Sicherheitslücken
Adobe hat zum Oktober-Patchday Sicherheitsupdates für neun Produkte veröffentlicht. Admins sollten sie zügig installieren.
- Link

—

Microsoft Patchday: Zwei Zeroday-Lücken werden bereits angegriffen
Zum Microsoft-Patchday im Oktober dichten die Entwickler auch zwei Sicherheitslücken ab, die bereits in freier Wildbahn angegriffen werden.
- Link

—

Kritische Sicherheitslücken in Draytek-Geräten erlauben Systemübernahme

Forscher fanden im Betriebssystem der Vigor-Router vierzehn neue Lücken, betroffen sind zwei Dutzend teilweise veraltete Typen. Patches stehen bereit.

- Link

—

SAP-Patchday: Sechs neu gemeldete Sicherheitslücken in Business-Software

Der Patchday im Oktober von SAP bringt wenige Aktualisierungen. Sechs Lücken stopfen die Entwickler neu, zwei davon sind hochriskant.

- Link

—

Android Patchday: System-Komponente ermöglicht Codeschmuggel aus dem Netz

Am Patchday im Oktober schließt Google mehrere Sicherheitslücken in Android. Die gravierendste ermöglicht Codeschmuggel aus dem Netz.

- 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	0.994860000	Link
CVE-2023-6895	0.927330000	0.990870000	Link
CVE-2023-6553	0.948430000	0.993340000	Link
CVE-2023-6019	0.933510000	0.991500000	Link
CVE-2023-52251	0.949200000	0.993460000	Link
CVE-2023-4966	0.970840000	0.998180000	Link
CVE-2023-49103	0.947620000	0.993230000	Link
CVE-2023-48795	0.964670000	0.996240000	Link
CVE-2023-47246	0.960640000	0.995360000	Link
CVE-2023-46805	0.960890000	0.995410000	Link
CVE-2023-46747	0.971910000	0.998540000	Link
CVE-2023-46604	0.971080000	0.998280000	Link
CVE-2023-4542	0.941060000	0.992350000	Link
CVE-2023-43208	0.974200000	0.999510000	Link
CVE-2023-43177	0.954700000	0.994400000	Link
CVE-2023-42793	0.970970000	0.998240000	Link
CVE-2023-41892	0.904950000	0.989110000	Link
CVE-2023-41265	0.907590000	0.989300000	Link
CVE-2023-39143	0.940700000	0.992300000	Link
CVE-2023-38205	0.951890000	0.993900000	Link
CVE-2023-38203	0.964750000	0.996290000	Link
CVE-2023-38146	0.919150000	0.990080000	Link
CVE-2023-38035	0.974600000	0.999680000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.967920000	0.997200000	Link
CVE-2023-3519	0.964810000	0.996300000	Link
CVE-2023-35082	0.967900000	0.997190000	Link
CVE-2023-35078	0.969440000	0.997620000	Link
CVE-2023-34993	0.973450000	0.999160000	Link
CVE-2023-34634	0.923140000	0.990470000	Link
CVE-2023-34362	0.970450000	0.998030000	Link
CVE-2023-34105	0.927500000	0.990900000	Link
CVE-2023-34039	0.943770000	0.992670000	Link
CVE-2023-3368	0.934610000	0.991620000	Link
CVE-2023-33246	0.970550000	0.998060000	Link
CVE-2023-32315	0.973230000	0.999080000	Link
CVE-2023-30625	0.953820000	0.994250000	Link
CVE-2023-30013	0.965950000	0.996640000	Link
CVE-2023-29300	0.967820000	0.997150000	Link
CVE-2023-29298	0.969430000	0.997620000	Link
CVE-2023-28432	0.921930000	0.990360000	Link
CVE-2023-28343	0.957650000	0.994870000	Link
CVE-2023-28121	0.922260000	0.990390000	Link
CVE-2023-27524	0.969670000	0.997700000	Link
CVE-2023-27372	0.973980000	0.999420000	Link
CVE-2023-27350	0.968980000	0.997480000	Link
CVE-2023-26469	0.953540000	0.994200000	Link
CVE-2023-26360	0.964630000	0.996230000	Link
CVE-2023-26035	0.967750000	0.997130000	Link
CVE-2023-25717	0.950620000	0.993660000	Link
CVE-2023-25194	0.964550000	0.996200000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963230000	0.995890000	Link
CVE-2023-24489	0.972860000	0.998930000	Link
CVE-2023-23752	0.949000000	0.993420000	Link
CVE-2023-23333	0.960430000	0.995300000	Link
CVE-2023-22527	0.970410000	0.998010000	Link
CVE-2023-22518	0.959950000	0.995240000	Link
CVE-2023-22515	0.973650000	0.999250000	Link
CVE-2023-21839	0.941470000	0.992400000	Link
CVE-2023-21554	0.952650000	0.994050000	Link
CVE-2023-20887	0.970950000	0.998230000	Link
CVE-2023-1698	0.917150000	0.989920000	Link
CVE-2023-1671	0.962220000	0.995670000	Link
CVE-2023-0669	0.971830000	0.998510000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Thu, 10 Oct 2024

[UPDATE] [hoch] Grub2: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

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

- Link

—

Thu, 10 Oct 2024

[UPDATE] [hoch] vim: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und Dateien zu manipulieren.

- Link

—

Thu, 10 Oct 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

—

Thu, 10 Oct 2024

[UPDATE] [hoch] Linux “Shim”: Schwachstelle ermöglicht Übernahme der Kontrolle

Ein anonymer Angreifer aus dem angrenzenden Netzwerk kann eine Schwachstelle in der “Shim” Komponente von Linux-Systemen ausnutzen, um die Kontrolle über ein betroffenes System zu übernehmen.

- Link

—

Thu, 10 Oct 2024

[UPDATE] [hoch] util-linux: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein lokaler Angreifer kann eine Schwachstelle in util-linux ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Thu, 10 Oct 2024

[UPDATE] [hoch] less: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in less ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 10 Oct 2024

[UPDATE] [hoch] Red Hat Enterprise Linux (shim): Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux in “shim” ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.

- Link

—

Thu, 10 Oct 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

—

Thu, 10 Oct 2024

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer oder ein lokaler authentifizierter Angreiferkann mehrere Schwachstellen in git ausnutzen, um beliebigen Programmcode auszuführen und und die Sicherheitsmaßnahmen zu umgehen.

- Link

—

Thu, 10 Oct 2024

[UPDATE] [hoch] Microsoft Visual Studio 2015: 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 Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022, Microsoft Visual Studio 2019, Microsoft Visual Studio 2022, Microsoft Visual C++ und Microsoft Windows ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen und einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Thu, 10 Oct 2024

[NEU] [hoch] Mitel MiCollab: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mitel MiCollab ausnutzen, um Dateien zu manipulieren, Sicherheitsmaßnahmen zu umgehen, Phishing-Angriffe durchzuführen und vertrauliche Informationen preiszugeben.

- Link

—

Thu, 10 Oct 2024

[NEU] [hoch] Juniper JUNOS: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Juniper JUNOS ausnutzen, um Denial-of-Service-Zustände herbeizuführen, Informationen preiszugeben, Code auszuführen, Privilegien zu erweitern und Sicherheitsmechanismen zu umgehen.

- Link

—

Thu, 10 Oct 2024

[NEU] [hoch] Progress Software Telerik Report Server: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Progress Software Telerik Report Server ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Thu, 10 Oct 2024

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

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

- Link

—

Thu, 10 Oct 2024

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

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

- Link

—

Thu, 10 Oct 2024

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

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

- Link

—

Thu, 10 Oct 2024

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

Ein entfernter, anonymer 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

—

Thu, 10 Oct 2024

[UPDATE] [hoch] Redis: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Redis ausnutzen, um einen Denial of Service Angriff durchzuführen oder Code auszuführen.

- Link

—

Thu, 10 Oct 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in CUPS cups-browsed ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Thu, 10 Oct 2024

[NEU] [hoch] Mozilla Firefox und ESR: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Mozilla Firefox und Mozilla Firefox ESR ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
10/9/2024	[Slackware Linux 15.0 / current mozilla-firefox Vulnerability (SSA:2024-283-01)]	critical
10/10/2024	[Fedora 40 : koji (2024-7ee01adadc)]	critical
10/10/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : mozjs78 (SUSE-SU-2024:3554-1)]	critical
10/10/2024	[openSUSE 15 Security Update : roundcubemail (openSUSE-SU-2024:0328-1)]	critical
10/10/2024	[RHEL 9 : firefox (RHSA-2024:7958)]	critical
10/10/2024	[FreeBSD : chromium – multiple security fixes (83117378-f773-4617-bf74-477d569dcd74)]	critical
10/10/2024	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : EDK II vulnerabilities (USN-7060-1)]	critical
10/10/2024	[Oracle Linux 8 : openssl (ELSA-2024-7848)]	critical
10/10/2024	[Debian dsa-5788 : firefox-esr - security update]	critical
10/10/2024	[Ubuntu 22.04 LTS : Go vulnerabilities (USN-7061-1)]	critical
10/10/2024	[AlmaLinux 8 : openssl (ALSA-2024:7848)]	critical
10/9/2024	[Oracle Linux 8 : .NET / 6.0 (ELSA-2024-7851)]	high

Datum	Schwachstelle	Bewertung
10/9/2024	[CBL Mariner 2.0 Security Update: oath-toolkit (CVE-2024-47191)]	high
10/10/2024	[SUSE SLED12 / SLES12 Security Update : kernel (SUSE-SU-2024:3559-1)]	high
10/10/2024	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2024:3564-1)]	high
10/10/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2024:3561-1)]	high
10/10/2024	[SUSE SLES15 Security Update : kernel (SUSE-SU-2024:3565-1)]	high
10/10/2024	[SUSE SLES15 / openSUSE 15 Security Update : redis (SUSE-SU-2024:3575-1)]	high
10/10/2024	[SUSE SLED15 / SLES15 Security Update : kernel (SUSE-SU-2024:3569-1)]	high
10/10/2024	[SUSE SLES12 Security Update : kernel (SUSE-SU-2024:3566-1)]	high
10/10/2024	[Oracle Linux 9 : .NET / 8.0 (ELSA-2024-7869)]	high
10/10/2024	[Oracle Linux 9 : .NET / 6.0 (ELSA-2024-7867)]	high
10/10/2024	[openSUSE 15 Security Update : seamonkey (openSUSE-SU-2024:0329-1)]	high
10/10/2024	[Juniper Junos OS Vulnerability (JSA88115)]	high
10/10/2024	[Juniper Junos OS Vulnerability (JSA88132)]	high
10/10/2024	[FreeBSD : powerdns-recursor – denial of service (8727b513-855b-11ef-9e50-6805ca2fa271)]	high
10/10/2024	[FreeBSD : Gitlab – vulnerabilities (cc1ac01e-86b0-11ef-9369-2cf05da270f3)]	high
10/10/2024	[FreeBSD : chromium – multiple security fixes (7217f6e8-3ff4-4387-845d-d1744bb7f95e)]	high
10/10/2024	[FreeBSD : gitea – token missing access control for packages (79b1f4ee-860a-11ef-b2dc-cbccbf25b7ea)]	high

Datum	Schwachstelle	Bewertung
10/10/2024	[Ubuntu 18.04 LTS : Linux kernel vulnerabilities (USN-7022-3)]	high
10/10/2024	[Oracle Linux 8 : .NET / 8.0 (ELSA-2024-7868)]	high
10/10/2024	[Oracle Linux 7 : systemd (ELSA-2024-7705)]	high
10/10/2024	[GitLab 17.1 < 17.2.9 / 17.3 < 17.3.5 / 17.4 < 17.4.2 (CVE-2024-6530)]	high
10/10/2024	[GitLab 15.10 < 17.2.9 / 17.3 < 17.3.5 / 17.4 < 17.4.2 (CVE-2024-8977)]	high
10/10/2024	[AlmaLinux 8 : .NET 8.0 (ALSA-2024:7868)]	high
10/10/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : libgsf vulnerabilities (USN-7062-1)]	high
10/10/2024	[Oracle Linux 7 : e2fsprogs (ELSA-2024-12730)]	high
10/10/2024	[Oracle Linux 7 : e2fsprogs (ELSA-2024-12731)]	high
10/10/2024	[AlmaLinux 8 : .NET 6.0 (ALSA-2024:7851)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Thu, 10 Oct 2024

ABB Cylon Aspect 3.08.01 persistenceManagerAjax.php Directory Traversal

ABB Cylon Aspect version 3.08.01 has a directory traversal vulnerability that can be exploited by an unauthenticated attacker to list the contents of arbitrary directories without reading file contents, leading to information disclosure of directory structures and filenames. This may expose sensitive system details, aiding in further attacks. The issue lies in the listFiles() function of the persistence-ManagerAjax.php script, which calls PHP’s readdir() function without proper input validation of the directory POST parameter.

- Link

—

” “Thu, 10 Oct 2024

Palo Alto Networks GlobalProtect Local Privilege Escalation

Palo Alto Networks GlobalProtect versions 5.1.x, 5.2.x, 6.0.x, 6.1.x, 6.3.x and versions less than 6.2.5

suffer from a local privilege escalation vulnerability.

- Link

—

” “Thu, 10 Oct 2024

Android GKI Kernels Use-After-Free

Android GKI kernels contain broken non-upstream Speculative Page Faults MM code that can lead to use-after-free conditions.

- Link

—

” “Wed, 09 Oct 2024

dav1d Integer Overflow / Out-Of-Bounds Write

There is an integer overflow in dav1d when decoding an AV1 video with large width/height. The integer overflow may result in an out-of-bounds write.

- Link

—

” “Tue, 08 Oct 2024

ABB Cylon Aspect 3.08.01 calendarFileDelete.php Arbitrary File Deletion

ABB Cylon Aspect version 3.08.01 suffers from an arbitrary file deletion vulnerability. Input passed to the file parameter in calendarFileDelete.php is not properly sanitized before being used to delete calendar files. This can be exploited by an unauthenticated attacker to delete files with the permissions of the web server using directory traversal sequences passed within the affected POST parameter.

- Link

—

” “Tue, 08 Oct 2024

PHP-Nuke Top Module SQL Injection

The Top module for PHP-Nuke versions 6.x and below 7.6 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 07 Oct 2024

Grav CMS 1.7.44 Server-Side Template Injection

GenGravSSTIExploit is a proof of concept Python script that exploits an authenticated server-side template injection (SSTI) vulnerability in Grav CMS versions 1.7.44 and below. This vulnerability allows a user with editor permissions to execute OS commands on a remote server.

- Link

—

” “Mon, 07 Oct 2024

Ruby-SAML / GitLab Authentication Bypass

This script exploits the issue noted in CVE-2024-45409 that allows an unauthenticated attacker with access to any signed SAML document issued by the IDP to forge a SAML Response/Assertion and gain access as any user on GitLab. Ruby-SAML versions below or equal to 12.2 and versions 1.13.0 through 1.16.0 do not properly verify the signature of the SAML Response.

- Link

—

” “Mon, 07 Oct 2024

iTunes For Windows 12.13.2.3 Local Privilege Escalation

This is a thorough write up of how to exploit a local privilege escalation vulnerability in iTunes for Windows version 12.13.2.3. Apple fixed this in version 12.13.3.

- Link

—

” “Mon, 07 Oct 2024

ABB Cylon Aspect 3.08.00 syslogSwitch.php Remote Code Execution

ABB Cylon Aspect versions 3.08.00 and below suffer from an authenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the SYSLOG HTTP POST parameter called by the syslogSwitch.php script.

- Link

—

” “Mon, 07 Oct 2024

ABB Cylon Aspect 3.08.01 caldavUtil.php Remote Code Execution

ABB Cylon Aspect versions 3.08.01 and below suffer from an unauthenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the Footer HTTP POST parameter called by the caldavUtil.php script.

- Link

—

” “Mon, 07 Oct 2024

ABB Cylon Aspect 3.08.00 setTimeServer.php Remote Code Execution

ABB Cylon Aspect versions 3.08.00 and below suffer from an authenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the timeserver HTTP POST parameter called by the setTimeServer.php script.

- Link

—

” “Mon, 07 Oct 2024

ABB Cylon Aspect 3.08.01 logYumLookup.php Unauthenticated File Disclosure

ABB Cylon Aspect versions 3.08.01 and below suffer from an unauthenticated arbitrary file disclosure vulnerability. Input passed through the logFile GET parameter via the logYumLookup.php script is not properly verified before being used to download log files. This can be exploited to disclose the con-

tents of arbitrary and sensitive files via directory traversal attacks.

- Link

—

” “Mon, 07 Oct 2024

Book Recording App 2024-09-24 Cross Site Scripting

Book Recording App, as submitted on 2024-09-24, suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Mon, 07 Oct 2024

OpenMediaVault 7.4.2-2 Code Injection

OpenMediaVault version 7.4.2-2 suffers from a PHP code injection vulnerability.

- Link

—

” “Mon, 07 Oct 2024

Netis MW5360 Code Injection

Netis MW5360 suffers from a PHP code injection vulnerability.

- Link

—

” “Mon, 07 Oct 2024

Hikvision IP Camera Cross Site Request Forgery

Hikvision IP Cameras suffer from a cross site request forgery vulnerability.

- Link

—

” “Mon, 07 Oct 2024

GeoServer 2.25.1 Code Injection

GeoServer version 2.25.1 suffers from a PHP code injection vulnerability.

- Link

—

” “Mon, 07 Oct 2024

Gambio Online Webshop 4.9.2.0 Code Injection

Gambio Online Webshop version 4.9.2.0 suffers from a PHP code injection vulnerability.

- Link

—

” “Fri, 04 Oct 2024

ABB Cylon Aspect 3.07.02 Authenticated File Disclosure

ABB Cylon Aspect version 3.07.02 suffers from an authenticated arbitrary file disclosure vulnerability. Input passed through the file GET parameter through the downloadDb.php script is not properly ve-

rified before being used to download database files. This can be exploited to disclose the contents of arbitrary and sensitive files via directory traversal attacks.

- Link

—

” “Fri, 04 Oct 2024

TeamViewer Privilege Escalation

Proof of concept code for a flaw in TeamViewer that enables an unprivileged user to load an arbitrary kernel driver into the system.

- Link

—

” “Fri, 04 Oct 2024

MD-Pro 1.0.76 Shell Upload / SQL Injection

MD-Pro version 1.0.76 suffers from remote SQL injection and shell upload vulnerabilities.

- Link

—

” “Fri, 04 Oct 2024

Computer Laboratory Management System 2024 1.0 Cross Site Scripting

Computer Laboratory Management System 2024 version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Fri, 04 Oct 2024

Acronis Cyber Infrastructure 5.0.1-61 Cross Site Request Forgery

Acronis Cyber Infrastructure version 5.0.1-61 suffers from a cross site request forgery vulnerability.

- Link

—

” “Fri, 04 Oct 2024

Vehicle Service Management System 1.0 WYSIWYG Code Injection

Vehicle Service Management System version 1.0 suffers from a WYSIWYG code injection vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Wed, 09 Oct 2024

ZDI-24-1333: NVIDIA Onyx Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1332: Adobe Dimension SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1331: Adobe Substance 3D Stager SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1330: Microsoft Windows win32kfull Use-After-Free Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1329: Axis Communications Autodesk Plugin AxisAddin axisapphelpfiles Remote Code Execution Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1328: Axis Communications Autodesk Plugin AzureBlobRestAPI axiscontentfiles Remote Code Execution Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1327: Ivanti Avalanche Faces ResourceManager Information Disclosure Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1326: Ivanti Avalanche SecureFilter allowPassThrough Authentication Bypass Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1325: Ivanti Avalanche SecureFilter Content-Type Authentication Bypass Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1324: Ivanti Avalanche validateAMCWSConnection Server-Side Request Forgery Information Disclosure Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1323: Centreon updateContactContactGroup SQL Injection Privilege Escalation Vulnerability

- Link

—

” “Tue, 08 Oct 2024

ZDI-24-1322: Centreon updateAccessGroupLinks SQL Injection Privilege Escalation Vulnerability

- Link

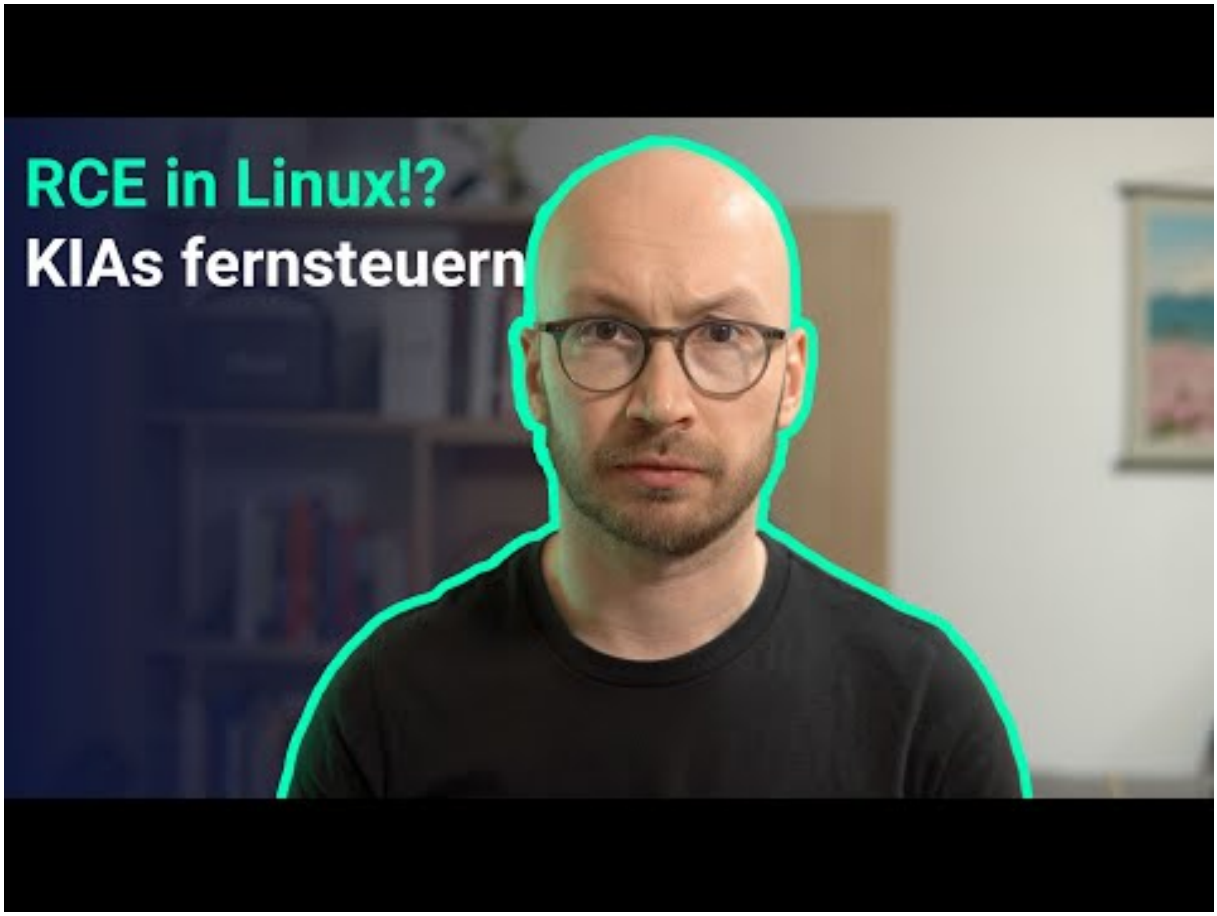
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Ein Grund mehr, Drucker zu hassen. Und Autos.



Zum Youtube Video

6 Cyberangriffe: (Okt)

Datum	Opfer	Land	Information
2024-10-08	Elbe-Heide	[DEU]	Link
2024-10-07	Vermilion Parish School System	[USA]	Link
2024-10-05	Casio Computer Co.	[JPN]	Link
2024-10-04	Groupe Hospi Grand Ouest	[FRA]	Link
2024-10-03	Uttarakhand	[IND]	Link
2024-10-03	American Water Works	[USA]	Link
2024-10-02	Thoraxzentrum Bezirk Unterfranken	[DEU]	Link
2024-10-02	Wayne County	[USA]	Link
2024-10-02	Traffics GmbH	[DEU]	Link
2024-10-01	Oyonnax	[FRA]	Link

7 Ransomware-Erpressungen: (Okt)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-10	[extramarks.com]	killsec	Link
2024-10-10	[Doctors Regional Cancer Center]	incransom	Link
2024-10-10	[oklahomasleepinstitute.co]	threeam	Link
2024-10-10	[Axis Health System]	rhysida	Link
2024-10-10	[The Law Office of Omar O Vargas]	meow	Link
2024-10-10	[Structural and Steel Products]	hunters	Link
2024-10-10	[medexhco.com]	ransomhub	Link
2024-10-10	[La Futura]	meow	Link
2024-10-10	[Barnes Cohen and Sullivan]	meow	Link
2024-10-10	[Atlantic Coast Consulting Inc]	meow	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-10	[Glacier]	hunters	Link
2024-10-09	[Casio Computer Co., Ltd]	underground	Link
2024-10-10	[Doscast]	handala	Link
2024-10-09	[FortyEighty Architecture]	play	Link
2024-10-09	[RobbJack & Crystallume]	play	Link
2024-10-09	[Universal Companies]	play	Link
2024-10-09	[argofinance.org]	killsec	Link
2024-10-09	[transfoodbeverage.com]	killsec	Link
2024-10-09	[InCare Technologies]	sarcoma	Link
2024-10-09	[Antenne Reunion Radio]	sarcoma	Link
2024-10-09	[Smart Media Group Bulgaria]	sarcoma	Link
2024-10-09	[The Roberts Family Law Firm]	sarcoma	Link
2024-10-09	[Gedco]	sarcoma	Link
2024-10-09	[EARTHWORKS Group]	sarcoma	Link
2024-10-09	[Perfection Fresh]	sarcoma	Link
2024-10-09	[Advanced Accounting & Business Advisory]	sarcoma	Link
2024-10-09	[Road Distribution Services]	sarcoma	Link
2024-10-09	[Lácteos Lorán]	sarcoma	Link
2024-10-09	[Curtidos Barbero]	sarcoma	Link
2024-10-09	[EasyPay]	sarcoma	Link
2024-10-09	[Jumbo Electronics Qatar]	sarcoma	Link
2024-10-09	[Navarra & Marzano]	sarcoma	Link
2024-10-09	[Costa Del Sol Hotels]	sarcoma	Link
2024-10-09	[The Plastic Bag]	sarcoma	Link
2024-10-09	[Elevator One]	sarcoma	Link
2024-10-09	[March Elevator]	sarcoma	Link
2024-10-09	[Suntrust Properties]	sarcoma	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-09	[tankstar.com]	lynx	Link
2024-10-09	[victrongroup.com]	abyss	Link
2024-10-09	[FULTON.COM]	clop	Link
2024-10-08	[Orbit Software, Inc.]	dragonforce	Link
2024-10-09	[avans.com]	killsec	Link
2024-10-08	[Eagle Recovery Associates]	play	Link
2024-10-08	[AnVa Industries]	play	Link
2024-10-08	[Smoker’s Choice]	play	Link
2024-10-08	[Saratoga Liquor]	play	Link
2024-10-08	[Accounting Resource Group]	play	Link
2024-10-08	[pingan.com]	killsec	Link
2024-10-08	[Ambassador of Israel in Germany Emails]	handala	Link
2024-10-08	[Aaren Scientific]	play	Link
2024-10-04	[blalockcompanies.com]	ransomhub	Link
2024-10-08	[Advantage CDC]	meow	Link
2024-10-08	[Trinity Wholesale Distributors Inc]	meow	Link
2024-10-08	[okcabstract.com]	ransomhub	Link
2024-10-08	[Blain Supply]	lynx	Link
2024-10-07	[Sit & Sleep]	lynx	Link
2024-10-08	[AIUT]	hunters	Link
2024-10-08	[Maxdream]	meow	Link
2024-10-08	[matki.co.uk]	cactus	Link
2024-10-08	[corporatejobbank.com]	cactus	Link
2024-10-08	[Davis Pickren Seydel and Sneed LLP]	meow	Link
2024-10-08	[Accurate Railroad Construction Ltd]	meow	Link
2024-10-08	[Max Shop]	handala	Link
2024-10-07	[autodoc.pro]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-07	[trulysmall.com]	ransomhub	Link
2024-10-07	[nspproteins.com]	ransomhub	Link
2024-10-07	[Richmond Auto Mall - Full Leak]	monti	Link
2024-10-08	[The Superior Court of California]	meow	Link
2024-10-08	[healthyuturn.in]	killsec	Link
2024-10-08	[uccretrievals.com]	ElDorado	Link
2024-10-08	[premierpackaging.com]	ElDorado	Link
2024-10-08	[htetech.com]	ElDorado	Link
2024-10-08	[goughconstruction.com]	ElDorado	Link
2024-10-08	[fleetequipment.com]	ElDorado	Link
2024-10-08	[auto-recyclers.com]	ElDorado	Link
2024-10-08	[atd-american.com]	ElDorado	Link
2024-10-08	[allianceind.com]	ElDorado	Link
2024-10-08	[avioesforza.it]	ElDorado	Link
2024-10-08	[tankerska.hr]	ElDorado	Link
2024-10-08	[totalelectronics.com]	ElDorado	Link
2024-10-07	[Istrail]	medusa	Link
2024-10-07	[Albany College of Pharmacy]	medusa	Link
2024-10-07	[Arelance Group]	medusa	Link
2024-10-08	[Pearl Cohen]	bianlian	Link
2024-10-07	[Broward Realty Corp]	everest	Link
2024-10-07	[yassir.com]	killsec	Link
2024-10-03	[tpgagedcare.com.au]	lockbit3	Link
2024-10-06	[IIB (Israeli Industrial Batteries) Leaked]	handala	Link
2024-10-03	[lyra.officegroup.it]	stormous	Link
2024-10-05	[AOSense/NASA]	stormous	Link
2024-10-05	[NASA/AOSense]	stormous	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-05	[Creative Consumer Concepts]	play	Link
2024-10-05	[Power Torque Services]	play	Link
2024-10-05	[seoulpi.io]	killsec	Link
2024-10-05	[canstarrestorations.com]	ransomhub	Link
2024-10-05	[www.ravencm.com]	ransomhub	Link
2024-10-05	[Ibermutuamur]	hunters	Link
2024-10-05	[betterhalf.ai]	killsec	Link
2024-10-05	[HARTSON-KENNEDY.COM]	clop	Link
2024-10-04	[omniboxx.nl]	ransomhub	Link
2024-10-05	[BNBuilders]	hunters	Link
2024-10-04	[winwinza.com]	ransomhub	Link
2024-10-04	[Storck-Baugesellschaft mbH]	incransom	Link
2024-10-04	[C&L Ward]	play	Link
2024-10-04	[Wilmington Convention Center]	play	Link
2024-10-04	[Guerriere & Halnon]	play	Link
2024-10-04	[Markdom Plastic Products]	play	Link
2024-10-04	[Pete’s Road Service]	play	Link
2024-10-04	[releese.io]	ransomhub	Link
2024-10-04	[kleberandassociates.com]	ransomhub	Link
2024-10-04	[City Of Forest Park - Full Leak]	monti	Link
2024-10-04	[Riley Gear Corporation]	akira	Link
2024-10-04	[TANYA Creations]	akira	Link
2024-10-04	[mullenwylie.com]	ElDorado	Link
2024-10-04	[GenPro Inc.]	blacksuit	Link
2024-10-04	[CopySmart LLC]	ciphbit	Link
2024-10-04	[North American Breaker]	akira	Link
2024-10-04	[Amplitude Laser]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-04	[GW Mechanical]	hunters	Link
2024-10-04	[Dreyfuss + Blackford Architecture]	hunters	Link
2024-10-04	[Transtec SAS]	orca	Link
2024-10-02	[enterpriseoutsourcing.com]	ransomhub	Link
2024-10-04	[DPC DATA]	qilin	Link
2024-10-03	[Lyomark Pharma]	dragonforce	Link
2024-10-03	[Conductive Containers, Inc]	cicada3301	Link
2024-10-04	[bbgc.gov.bd]	killsec	Link
2024-10-03	[CobelPlast]	hunters	Link
2024-10-03	[Shin Bet]	handala	Link
2024-10-03	[Barnes & Cohen]	trinity	Link
2024-10-03	[TRC Worldwide Engineering (Trcww)]	akira	Link
2024-10-03	[Rob Levine & Associates (roblevine.com)]	akira	Link
2024-10-03	[Red Barrels]	nitrogen	Link
2024-10-03	[CaleyWray]	hunters	Link
2024-10-03	[LIFTING.COM]	clop	Link
2024-10-01	[Emerson]	medusa	Link
2024-10-03	[Golden Age Nursing Home]	rhysida	Link
2024-10-02	[domainindustries.com]	ransomhub	Link
2024-10-02	[ironmetals.com]	ransomhub	Link
2024-10-02	[rollxvans.com]	ransomhub	Link
2024-10-02	[ETC Companies]	akira	Link
2024-10-02	[Branhaven Chrysler Dodge Jeep Ram]	blacksuit	Link
2024-10-02	[Holmes & Brakel]	akira	Link
2024-10-02	[Forshey Prostok LLP]	qilin	Link
2024-10-02	[Israel Prime Minister Emails]	handala	Link
2024-10-02	[FoccoERP]	trinity	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-01	[Quantum Healthcare]	incransom	Link
2024-10-01	[United Animal Health]	qilin	Link
2024-10-01	[Akromold]	nitrogen	Link
2024-10-01	[Labib Funk Associates]	nitrogen	Link
2024-10-01	[Research Electronics International]	nitrogen	Link
2024-10-01	[Cascade Columbia Distribution]	akira	Link
2024-10-01	[ShoreMaster]	akira	Link
2024-10-01	[marthamedeiros.com.br]	madliberator	Link
2024-10-01	[CSG Consultants]	akira	Link
2024-10-01	[aberdeenwa.gov]	ElDorado	Link
2024-10-01	[Corantioquia]	meow	Link
2024-10-01	[performance-therapies]	qilin	Link
2024-10-01	[www.galab.com]	cactus	Link
2024-10-01	[telehealthcenter.in]	killsec	Link
2024-10-01	[howardcpas.com]	ElDorado	Link
2024-10-01	[bshsoft.com]	ElDorado	Link
2024-10-01	[credihealth.com]	killsec	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.