Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241004

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

Zimbra: Codeschmuggel-Lücke wird angegriffen

In der Kollaborationssoftware Zimbra klafft eine Sicherheitslücke, die Angreifer bereits aktiv missbrauchen. Admins sollten zügig updaten.

- Link

—

Web-Config von Seiko-Epson-Geräten ermöglicht Angreifern Übernahme

Das Web-Interface von Geräten wie Druckern von Seiko-Epson ermöglicht Angreifern in vielen Fällen, diese als Administrator zu übernehmen.

- Link

—

CERT-Bund warnt: Mehr als 15.000 Exchange-Server mit Sicherheitslücken

In Deutschland stehen noch immer mehr als 15.000 Exchange-Server mit mindestens einer Codeschmuggel-Lücke offen im Netz, warnt das CERT-Bund.

- Link

—

Monitoring-Software Whatsup Gold: Hersteller rät zum schleunigen Update

Progress warnt, dass teils kritische Sicherheitslücken in Whatsup Gold lauern. Admins sollen so schnell wie möglich aktualisieren.

- Link

—

Kritische Sicherheitslücken: PHP 8.3.12, 8.2.24 und 8.1.30 dichten Lecks ab

Die PHP-Entwickler haben PHP 8.3.12, 8.2.24 und 8.1.30 veröffentlicht. Darin schließen sie mehrere, teils kritische Sicherheitslücken.

- Link

—

Foxit PDF: Manipulierte PDFs können Schadcode durchschleusen

Es sind gegen verschiedene Attacken gerüstete Versionen von Foxit PDF Editor und PDF Reader für macOS und Windows erschienen.

- Link

—

Teils kritische Lücken in Unix-Drucksystem CUPS ermöglichen Codeschmuggel

Im Linux-Drucksystem CUPS wurden teils kritische Sicherheitslücken entdeckt. Angreifer können dadurch etwa Code einschmuggeln.

- Link

—

Schadcode-Schlupfloch in Nvidia Container Toolkit geschlossen

Angreifer können an Sicherheitslücken in Nvidia Container Toolkit und GPU Operator ansetzen, um Systeme zu kompromittieren.

- Link

—

Sicherheitsupdates: DoS-Angriffe auf Cisco-Netzwerkhardware möglich

Aufgrund von mehreren Sicherheitslücken in Ciscos Netzwerkbetriebssystem IOS XE sind verschiedene Geräte verwundbar. Patches stehen zum Download.

- Link

—

Progress Telerik: hochriskante Lücken erlauben Code- und Befehlsschmuggel

In Progress Telerik UI for WPF und WinForms können Angreifer aufgrund von Sicherheitslücken Schadcode und Befehle einschmuggeln.

- 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	0.994820000	Link
CVE-2023-6895	0.927330000	0.990820000	Link
CVE-2023-6553	0.947820000	0.993190000	Link
CVE-2023-6019	0.918710000	0.989980000	Link
CVE-2023-52251	0.949200000	0.993400000	Link
CVE-2023-4966	0.970840000	0.998160000	Link
CVE-2023-49103	0.949680000	0.993490000	Link
CVE-2023-48795	0.964670000	0.996200000	Link
CVE-2023-47246	0.960360000	0.995250000	Link
CVE-2023-46805	0.960890000	0.995380000	Link
CVE-2023-46747	0.971540000	0.998420000	Link
CVE-2023-46604	0.970850000	0.998170000	Link
CVE-2023-4542	0.944110000	0.992640000	Link
CVE-2023-43208	0.974060000	0.999430000	Link
CVE-2023-43177	0.958390000	0.994950000	Link
CVE-2023-42793	0.970970000	0.998220000	Link
CVE-2023-41892	0.904950000	0.989060000	Link
CVE-2023-41265	0.907590000	0.989240000	Link
CVE-2023-39143	0.940700000	0.992230000	Link
CVE-2023-38205	0.951890000	0.993850000	Link
CVE-2023-38203	0.964750000	0.996250000	Link
CVE-2023-38146	0.919150000	0.990030000	Link
CVE-2023-38035	0.974550000	0.999670000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.967920000	0.997180000	Link
CVE-2023-3519	0.965910000	0.996600000	Link
CVE-2023-35082	0.967900000	0.997170000	Link
CVE-2023-35078	0.969440000	0.997620000	Link
CVE-2023-34993	0.973450000	0.999160000	Link
CVE-2023-34960	0.900520000	0.988790000	Link
CVE-2023-34634	0.923140000	0.990410000	Link
CVE-2023-34362	0.970450000	0.998010000	Link
CVE-2023-34105	0.927500000	0.990840000	Link
CVE-2023-34039	0.943770000	0.992590000	Link
CVE-2023-3368	0.942240000	0.992390000	Link
CVE-2023-33246	0.969870000	0.997800000	Link
CVE-2023-32315	0.971490000	0.998400000	Link
CVE-2023-30625	0.953820000	0.994230000	Link
CVE-2023-30013	0.965950000	0.996620000	Link
CVE-2023-29300	0.967820000	0.997130000	Link
CVE-2023-29298	0.969430000	0.997610000	Link
CVE-2023-28432	0.921930000	0.990300000	Link
CVE-2023-28343	0.937460000	0.991870000	Link
CVE-2023-28121	0.922260000	0.990340000	Link
CVE-2023-27524	0.970600000	0.998060000	Link
CVE-2023-27372	0.974150000	0.999480000	Link
CVE-2023-27350	0.968980000	0.997470000	Link
CVE-2023-26469	0.953540000	0.994170000	Link
CVE-2023-26360	0.964630000	0.996190000	Link
CVE-2023-26035	0.967750000	0.997110000	Link
CVE-2023-25717	0.950620000	0.993620000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-25194	0.964550000	0.996160000	Link
CVE-2023-2479	0.963230000	0.995840000	Link
CVE-2023-24489	0.972860000	0.998920000	Link
CVE-2023-23752	0.952050000	0.993890000	Link
CVE-2023-23333	0.960430000	0.995270000	Link
CVE-2023-22527	0.970500000	0.998030000	Link
CVE-2023-22518	0.959950000	0.995210000	Link
CVE-2023-22515	0.973910000	0.999360000	Link
CVE-2023-21839	0.947720000	0.993180000	Link
CVE-2023-21554	0.952650000	0.994020000	Link
CVE-2023-20887	0.970950000	0.998220000	Link
CVE-2023-1698	0.917150000	0.989850000	Link
CVE-2023-1671	0.962220000	0.995620000	Link
CVE-2023-0669	0.971830000	0.998500000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 02 Oct 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

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

- Link

—

Wed, 02 Oct 2024

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

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen oder Daten zu manipulieren.

- Link

—

Wed, 02 Oct 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, 02 Oct 2024

[NEU] [hoch] Google Chrome: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

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

- Link

—

Wed, 02 Oct 2024

[UPDATE] [hoch] Mehrere DNS Server: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in mehreren DNS Server Produkten ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Wed, 02 Oct 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Firefox ESR ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmechanismen zu umgehen, Daten zu manipulieren und den Benutzer zu täuschen.

- Link

—

Wed, 02 Oct 2024

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

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um einen Spoofing-Angriff durchzuführen, beliebigen Code auszuführen, Dateien zu manipulieren, vertrauliche Informationen offenzulegen oder Cross-Site-Scripting-Angriffe durchzuführen.

- Link

—

Wed, 02 Oct 2024

[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen

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

- Link

—

Wed, 02 Oct 2024

[UPDATE] [hoch] Mozilla Firefox, 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, Sicherheitsmaßnahmen zu umgehen oder Daten zu manipulieren.

- Link

—

Wed, 02 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

—

Wed, 02 Oct 2024

[UPDATE] [kritisch] PHP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um beliebigen Programmcode auszuführen, Informationen preiszugeben und andere nicht spezifizierte Angriffe durchzuführen.

- Link

—

Wed, 02 Oct 2024

[NEU] [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

—

Wed, 02 Oct 2024

[UPDATE] [hoch] Octopus Deploy: Schwachstelle ermöglicht SQL Injection

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Octopus Deploy ausnutzen, um

einen SQL Injection Angriff durchzuführen.
- Link

—

Tue, 01 Oct 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

—

Tue, 01 Oct 2024

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

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

—

Tue, 01 Oct 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

—

Tue, 01 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

—

Tue, 01 Oct 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.
- Link

—

Tue, 01 Oct 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation

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

- Link

—

Tue, 01 Oct 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

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
10/3/2024	[GitHub Enterprise 3.10.x < 3.10.16 / 3.11.x < 3.11.14 / 3.12.x < 3.12.8 / 3.13.x < 3.13.3 (ghsa_5wm9_5344_qrrj)]	critical
10/3/2024	[Ubuntu 14.04 LTS : ImageMagick vulnerabilities (USN-7053-1)]	critical
10/3/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : FreeRADIUS vulnerability (USN-7055-1)]	critical
10/3/2024	[Oracle Linux 9 : thunderbird (ELSA-2024-7552)]	critical
10/3/2024	[Debian dla-3909 : zabbix-agent - security update]	critical
10/3/2024	[Microsoft Edge (Chromium) < 129.0.2792.79 Multiple Vulnerabilities]	critical
10/3/2024	[Amazon Linux 2 : amazon-ssm-agent (ALAS-2024-2645)]	critical
10/3/2024	[Amazon Linux 2 : thunderbird (ALAS-2024-2638)]	critical
10/3/2024	[Ubuntu 16.04 LTS : GNOME Shell vulnerabilities (USN-7052-1)]	high
10/3/2024	[RHEL 8 : cups-filters (RHSA-2024:7623)]	high
10/3/2024	[RHEL 9 : firefox (RHSA-2024:7622)]	high
10/3/2024	[RHEL 9 : firefox (RHSA-2024:7621)]	high

Datum	Schwachstelle	Bewertung
10/3/2024	[NVIDIA Container Toolkit < 1.16.2 Multiple Vulnerabilities]	high
10/3/2024	[Jenkins plugins Multiple Vulnerabilities (2024-10-02)]	high
10/3/2024	[Debian dsa-5782 : affs-modules-6.1.0-22-4kc-malta-di - security update]	high
10/3/2024	[Amazon Linux 2 : python-setuptools (ALAS-2024-2641)]	high
10/3/2024	[Amazon Linux 2023 : redis6, redis6-devel (ALAS2023-2024-717)]	high
10/3/2024	[Amazon Linux 2 : python-dns (ALAS-2024-2647)]	high
10/3/2024	[Amazon Linux 2 : kernel (ALAS-2024-2642)]	high
10/3/2024	[Amazon Linux 2 : golang (ALAS-2024-2643)]	high
10/3/2024	[Amazon Linux 2 : thunderbird (ALAS-2024-2640)]	high
10/3/2024	[Amazon Linux 2 : xerces-j2 (ALAS-2024-2649)]	high
10/3/2024	[Amazon Linux 2 : libtiff (ALAS-2024-2639)]	high
10/3/2024	[RHEL 8 : python3.11 (RHSA-2024:7647)]	high
10/3/2024	[RHEL 8 : firefox (RHSA-2024:7646)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Thu, 03 Oct 2024

Acronis Cyber Infrastructure Default Password Remote Code Execution

Acronis Cyber Infrastructure (ACI) is an IT infrastructure solution that provides storage, compute, and network resources. Businesses and Service Providers are using it for data storage, backup storage, creating and managing virtual machines and software-defined networks, running cloud-native applications in production environments. This Metasploit module exploits a default password vulnerability in ACI which allow an attacker to access the ACI PostgreSQL database and gain administrative access to the ACI Web Portal. This opens the door for the attacker to upload SSH keys that enables root access to the appliance/server. This attack can be remotely executed over the WAN as long as the PostgreSQL and SSH services are exposed to the outside world. ACI versions 5.0 before build 5.0.1-61, 5.1 before build 5.1.1-71, 5.2 before build 5.2.1-69, 5.3 before build 5.3.1-53, and 5.4 before build 5.4.4-132 are

vulnerable.

- Link

—

” “Thu, 03 Oct 2024

dizqueTV 1.5.3 Remote Code Execution

dizqueTV version 1.5.3 suffers from a remote code execution vulnerability.

- Link

—

” “Thu, 03 Oct 2024

openSIS 9.1 SQL Injection

openSIS version 9.1 suffers from a remote SQL injection vulnerability.

- Link

—

” “Thu, 03 Oct 2024

reNgine 2.2.0 Command Injection

reNgine version 2.2.0 suffers from an authenticated command injection vulnerability.

- Link

—

” “Thu, 03 Oct 2024

WordPress Bricks Builder Theme 1.9.6 Code Injection

WordPress Bricks Builder Theme version 1.9.6 suffers from a PHP code injection vulnerability.

- Link

—

” “Thu, 03 Oct 2024

WordPress Hash Form 1.1.0 Code Injection

WordPress Hash Form plugin version 1.1.0 suffers from a PHP code injection vulnerability.

- Link

—

” “Thu, 03 Oct 2024

WordPress GiveWP Donation Fundraising Platform 3.14.1 Code Injection

WordPress GiveWP Donation Fundraising Platform version 3.14.1 suffers from a PHP code injection vulnerability.

- Link

—

” “Thu, 03 Oct 2024

ViciDial 2.0.5 Cross Site Request Forgery

ViciDial version 2.0.5 suffers from a cross site request forgery vulnerability.

- Link

—

” “Thu, 03 Oct 2024

Vehicle Service Management System 1.0 Cross Site Request Forgery

Vehicle Service Management System version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Thu, 03 Oct 2024

Transport Management System 1.0 Insecure Direct Object Reference

Transport Management System version 1.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Thu, 03 Oct 2024

Printing Business Records Management System 1.0 Insecure Settings

Printing Business Records Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Thu, 03 Oct 2024

Online Eyewear Shop 1.0 Insecure Settings

Online Eyewear Shop version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Thu, 03 Oct 2024

AVideo 12.4 Code Injection

AVideo version 12.4 suffers from a PHP code injection vulnerability.

- Link

—

” “Wed, 02 Oct 2024

CUPS Arbitrary Command Execution

Proof of concept remote command execution exploit for CUPS that leverages the vulnerability outlined in CVE-2024-47176.

- Link

—

” “Wed, 02 Oct 2024

ALEOS 4.16 Denial Of Service

ALEOS versions 4.16 and below denial of service proof of concept exploit.

- Link

—

” “Wed, 02 Oct 2024

SeedDMS 6.0.28 Cross Site Scripting

SeedDMS version 6.0.28 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Wed, 02 Oct 2024

Microsoft Office NTLMv2 Disclosure

Microsoft Office 2019 MSO build 1808 (16.0.10411.20011) and Microsoft 365 MSO version 2403 build 16.0.17425.20176 suffer from an NTLMv2 hash disclosure vulnerability.

- Link

—

” “Wed, 02 Oct 2024

Tourism Management System 1.0 Cross Site Scripting

Tourism Management System version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Wed, 02 Oct 2024

TitanNit Web Control 2.01 / Atemio 7600 Code Injection

TitanNit Web Control 2.01 and Atemio 7600 suffer from a PHP code injection vulnerability.

- Link

—

” “Wed, 02 Oct 2024

Teacher Subject Allocation Management System 1.0 Insecure Settings

Teacher Subject Allocation Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Wed, 02 Oct 2024

Task Management System 1.0 Code Injection

Task Management System version 1.0 suffers from a PHP code injection vulnerability.

- Link

—

” “Wed, 02 Oct 2024

Supply Chain Management 1.0 Backup Disclosure

Supply Chain Management version 1.0 suffers from a backup disclosure vulnerability.

- Link

—

” “Wed, 02 Oct 2024

Event Management System 1.0 Insecure Direct Object Reference

Event Management System version 1.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Wed, 02 Oct 2024

Student Attendance Management System 1.0 Insecure Settings

Student Attendance Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Wed, 02 Oct 2024

Printing Business Records Management System 1.0 Cross Site Request Forgery

Printing Business Records Management System version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Wed, 02 Oct 2024

ZDI-24-1321: Apple macOS AppleVADriver Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Wed, 02 Oct 2024

ZDI-24-1320: Autodesk Navisworks Freedom DWF File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Wed, 02 Oct 2024

ZDI-24-1319: Autodesk Navisworks Freedom DWF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Wed, 02 Oct 2024

ZDI-24-1318: Autodesk Navisworks Freedom DWFX File Parsing Out-Of-Bounds Write Remote Code

Execution Vulnerability

- Link

—

” “Wed, 02 Oct 2024

ZDI-24-1317: Autodesk Navisworks Freedom DWFX File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Wed, 02 Oct 2024

ZDI-24-1316: Autodesk Navisworks Freedom DWFX File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Wed, 02 Oct 2024

ZDI-24-1315: Autodesk Navisworks Freedom DWF File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Wed, 02 Oct 2024

ZDI-24-1314: PaperCut NG pc-web-print Link Following Denial-of-Service Vulnerability

- Link

—

” “Wed, 02 Oct 2024

ZDI-24-1313: Apple macOS ImageIO PSD File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Wed, 02 Oct 2024

ZDI-24-1312: Apple macOS ImageIO KTX Image Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Wed, 02 Oct 2024

ZDI-24-1311: Microsoft Windows Menu DC Path Use-After-Free Local Privilege Escalation Vulnerability

- Link

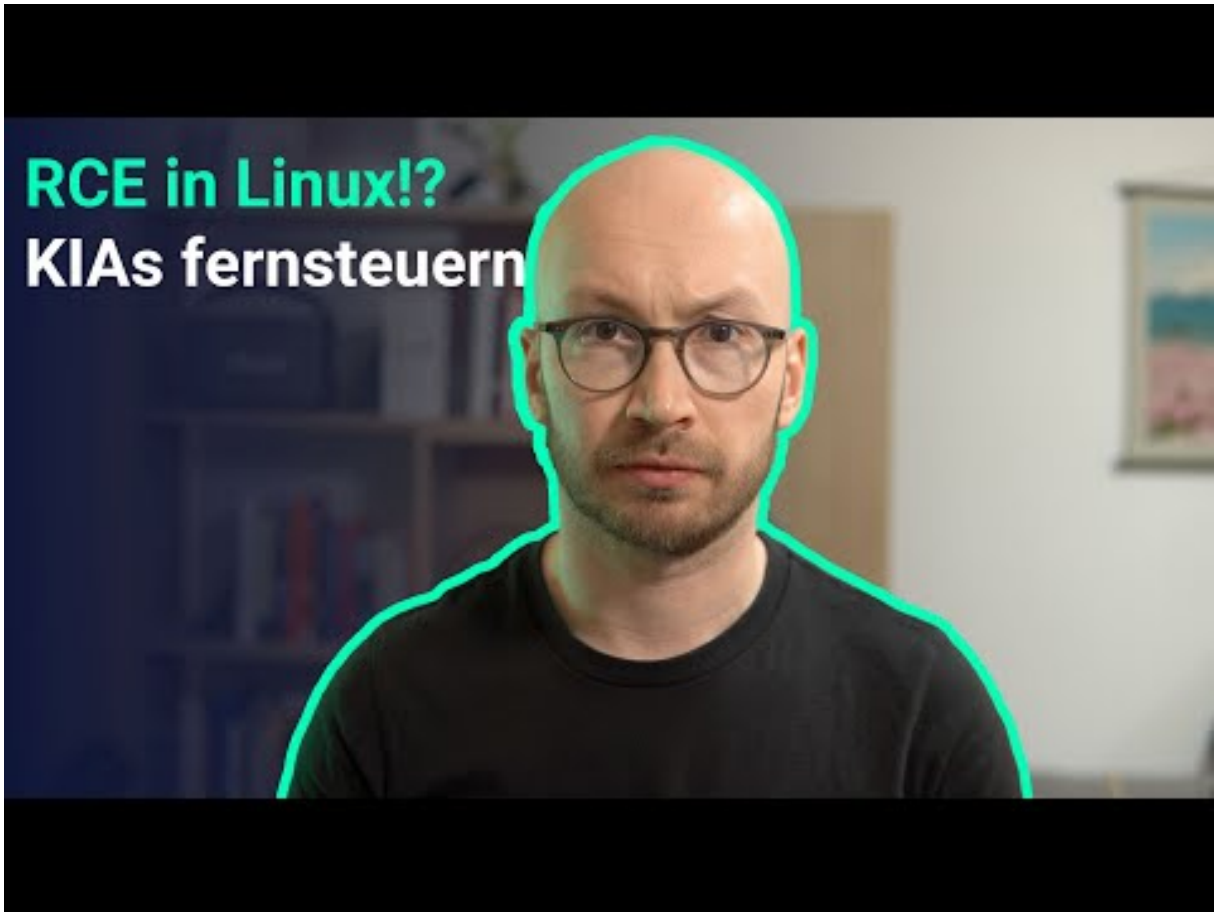
—

”

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
2024-10-02	Thoraxzentrum Bezirk Unterfranken	[DEU]	Link
2024-10-02	Wayne County	[USA]	Link

7 Ransomware-Erpressungen: (Okt)

Datum	Opfer	Ransomware-Grupppe	Webseite
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	[mccartycompany.com]	ransomhub	Link
2024-10-02	[bypeterandpauls.com]	ransomhub	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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-10-01	[Quantum Healthcare]	incransom	Link
2024-10-01	[Acuity Advisor]	stormous	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.