Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240905

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

Android Patchday: Updates schließen mehrere hochriskante Lücken

Im September gibt Google zum Patchday fehlerbereinigte Android-Versionen heraus. Sie schließen vor allem hochriskante Lücken.

- Link

—

Zyxel: Mehrere hochriskante Sicherheitslücken in Firewalls

Zyxel warnt vor mehreren Sicherheitslücken in den Firewalls des Unternehmens. Updates stehen bereit, die Lecks abdichten.

- Link

—

VMware Fusion: Update stopft Rechteausweitungslücke

Broadcom schließt mit einem Update eine Sicherheitslücke in VMware Fusion. Angreifer können ihre Rechte dadurch ausweiten.

- Link

—

“Whatsup Gold”: Umgehen der Anmeldung durch kritische Sicherheitslücken möglich

Progress schließt mit aktualisierter Software kritische Sicherheitslücken in der Monitoring-Software “Whatsup Gold”.

- Link

—

Support ausgelaufen: Attacken auf IP-Kamera von Avtech beobachtet

Derzeit attackiert das Corona-Mirai-Botnet die IP-Kamera AVM1203 von Avtech. Die Kamera wird in öffentlichen Einrichtungen und Industrieanlagen verwendet.

- Link

—

BIOS-Update: Angreifer können Secure Boot auf Alienware-Notebooks umgehen

Unter bestimmten Voraussetzungen können Angreifer eine zentrale Schutzfunktion von Dells Alienware-Notebooks umgehen.

- Link

—

Fortra FileCatalyst Workflow: Hintertür macht Angreifer zu Admins

Aufgrund von hartkodierten Zugangsdaten können sich Angreifer weitreichenden Zugriff auf Fortra FileCatalyst Workflow verschaffen.

- Link

—

Sicherheitsupdates: Cisco Switches sind für DoS-Attacken anfällig

Es sind wichtige Sicherheitsupdates für verschiedene Produkte des Netzwerkausrüsters Cisco erscheinen.

- Link

—

Hitachi Ops Center: Attacken auf Hitachi-Speicherinfrastruktur möglich

Hitachi Ops Center Common Services ist unter Linux verwundbar. Eine abgesicherte Version ist erschienen.

- Link

—

Ticketsystem OTRS: Angreifer können unverschlüsselte Passwörter einsehen

Die Entwickler des Open Ticket Request System haben mehrere Sicherheitslücken geschlossen.

- Link

—

3 Sicherheitslücken

Eine Sicherheitslücke oder Schwachstelle ist ein Fehler in einer Software oder Hardware, der es einem Angreifer ermöglicht, in ein Computersystem einzudringen und Schaden anzurichten. Diese Lücke stellt eine Bedrohung für die Sicherheit des Systems dar, da sie ausgenutzt werden kann, um das System zu kompromittieren. Sicherheitslücken entstehen oft durch unzureichenden Schutz des Computers vor Netzwerkangriffen, zum Beispiel durch fehlende Firewall oder andere Sicherheitssoftware. Auch Programmierfehler im Betriebssystem, Webbrowser oder anderen Anwendungen können Sicherheitslücken verursachen. Bekannte Sicherheitslücken sollten daher so schnell wie möglich durch das Einspielen eines Patches geschlossen werden, um die Angriffsfläche der IT-Systeme zu verringern.

3.1 EPSS

Das Exploit Prediction Scoring System wird für eine bekannte Software-Sicherheitslücke / CVE auf einer Skala von 0 (0%) bis 1 (100%) angegeben und soll die Wahrscheinlichkeit für das Auftreten eines Exploits in naher Zukunft darstellen. Ein höherer Wert bedeutet eine höhere Wahrscheinlichkeit, dass eine Schwachstelle in naher Zukunft ausgenutzt wird. EPSS kann auch als Rahmen für die Priorisierung von Schwachstellen unter Verwendung einer Kombination von Metriken betrachtet werden.

Es soll Unternehmen dabei helfen, ihre Ressourcen effizienter zu verteilen und alle relevanten Cyber-Risiken zu minimieren.

3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-7028	0.957050000	0.994750000	Link
CVE-2023-6895	0.921160000	0.990150000	Link
CVE-2023-6553	0.937150000	0.991780000	Link
CVE-2023-6019	0.918710000	0.989890000	Link
CVE-2023-5360	0.902780000	0.988870000	Link
CVE-2023-52251	0.946410000	0.992900000	Link
CVE-2023-4966	0.970940000	0.998180000	Link
CVE-2023-49103	0.964700000	0.996220000	Link
CVE-2023-48795	0.965330000	0.996450000	Link
CVE-2023-47246	0.959760000	0.995180000	Link
CVE-2023-46805	0.950230000	0.993550000	Link
CVE-2023-46747	0.972260000	0.998640000	Link
CVE-2023-46604	0.968800000	0.997420000	Link
CVE-2023-4542	0.948590000	0.993270000	Link
CVE-2023-43208	0.973970000	0.999380000	Link
CVE-2023-43177	0.961750000	0.995560000	Link
CVE-2023-42793	0.971190000	0.998300000	Link
CVE-2023-41265	0.907590000	0.989170000	Link
CVE-2023-39143	0.940480000	0.992160000	Link
CVE-2023-38205	0.953670000	0.994160000	Link
CVE-2023-38203	0.965830000	0.996600000	Link
CVE-2023-38146	0.920720000	0.990100000	Link
CVE-2023-38035	0.974690000	0.999730000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.966750000	0.996860000	Link
CVE-2023-3519	0.965910000	0.996620000	Link
CVE-2023-35082	0.967460000	0.997060000	Link
CVE-2023-35078	0.970450000	0.997960000	Link
CVE-2023-34993	0.973540000	0.999190000	Link
CVE-2023-34960	0.921610000	0.990220000	Link
CVE-2023-34634	0.923140000	0.990350000	Link
CVE-2023-34362	0.970450000	0.997960000	Link
CVE-2023-34039	0.947070000	0.993020000	Link
CVE-2023-3368	0.942130000	0.992340000	Link
CVE-2023-33246	0.967180000	0.996970000	Link
CVE-2023-32315	0.970220000	0.997880000	Link
CVE-2023-30625	0.953610000	0.994150000	Link
CVE-2023-30013	0.965950000	0.996630000	Link
CVE-2023-29300	0.969240000	0.997560000	Link
CVE-2023-29298	0.969880000	0.997760000	Link
CVE-2023-28432	0.907350000	0.989150000	Link
CVE-2023-28343	0.933130000	0.991420000	Link
CVE-2023-28121	0.919520000	0.989980000	Link
CVE-2023-27524	0.970600000	0.998010000	Link
CVE-2023-27372	0.973470000	0.999170000	Link
CVE-2023-27350	0.968480000	0.997320000	Link
CVE-2023-26469	0.951470000	0.993750000	Link
CVE-2023-26360	0.964390000	0.996140000	Link
CVE-2023-26035	0.969020000	0.997470000	Link
CVE-2023-25717	0.954250000	0.994260000	Link
CVE-2023-25194	0.966980000	0.996930000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963960000	0.996040000	Link
CVE-2023-24489	0.973820000	0.999310000	Link
CVE-2023-23752	0.956380000	0.994630000	Link
CVE-2023-23333	0.961070000	0.995420000	Link
CVE-2023-22527	0.970940000	0.998190000	Link
CVE-2023-22518	0.965200000	0.996390000	Link
CVE-2023-22515	0.972760000	0.998880000	Link
CVE-2023-21839	0.955020000	0.994390000	Link
CVE-2023-21554	0.955880000	0.994560000	Link
CVE-2023-20887	0.970840000	0.998130000	Link
CVE-2023-1671	0.962690000	0.995720000	Link
CVE-2023-0669	0.971330000	0.998370000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 04 Sep 2024

[NEU] [hoch] Android Patchday September: Mehrere Schwachstellen

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu erzeugen oder vertrauliche Informationen offenzulegen.

- Link

—

Wed, 04 Sep 2024

[NEU] [hoch] Apache OFBiz: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache OFBiz ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder vertrauliche Informationen offenzulegen.

- Link

—

Wed, 04 Sep 2024

[NEU] [hoch] Pixel Patchday September 2024: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um seine Privilegien zu erhöhen oder Informationen offenzulegen.
- Link

—

Wed, 04 Sep 2024

[NEU] [hoch] Kemp LoadMaster: Schwachstelle ermöglicht Ausführen von beliebigen Kommandos

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Kemp LoadMaster ausnutzen, um beliebige Systemkommandos auszuführen.
- Link

—

Wed, 04 Sep 2024

[NEU] [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, 04 Sep 2024

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

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

—

Wed, 04 Sep 2024

[UPDATE] [hoch] zlib: Schwachstelle ermöglicht nicht spezifizierten Angriff

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in zlib ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.
- Link

—

Wed, 04 Sep 2024

[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

Wed, 04 Sep 2024

[UPDATE] [hoch] PostgreSQL: Mehrere Schwachstellen

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um Informationen offenzulegen, beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Wed, 04 Sep 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Logback ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Wed, 04 Sep 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Logback ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Wed, 04 Sep 2024

[UPDATE] [hoch] Red Hat Advanced Cluster Management for Kubernetes: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen im Red Hat Advanced Cluster Management for Kubernetes ausnutzen, um einen Denial of Service Angriff durchzuführen oder beliebigen Code auszuführen.

- Link

—

Wed, 04 Sep 2024

[UPDATE] [hoch] docker: Mehrere Schwachstellen

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

- Link

—

Wed, 04 Sep 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

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

- Link

—

Wed, 04 Sep 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Podman ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 04 Sep 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

—

Wed, 04 Sep 2024

[UPDATE] [hoch] ffmpeg: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in ffmpeg ausnutzen, um beliebigen Code auszuführen oder einen 'Denial of Service'-Zustand zu verursachen.

- Link

—

Wed, 04 Sep 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder einen 'Denial of Service'-Zustand zu verursachen.

- Link

—

Wed, 04 Sep 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

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

- Link

—

Wed, 04 Sep 2024

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

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

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/4/2024	[SUSE SLES15 / openSUSE 15 Security Update : buildah, docker (SUSE-SU-2024:3120-1)]	critical
9/4/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : go1.21-openssl (SUSE-SU-2024:3089-1)]	critical
9/4/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaThunderbird (SUSE-SU-2024:3112-1)]	critical
9/4/2024	[SUSE SLES15 / openSUSE 15 Security Update : openssl-1_0_0 (SUSE-SU-2024:3119-1)]	critical
9/4/2024	[Debian dla-3869 : firefox-esr - security update]	critical
9/4/2024	[RHEL 8 : Satellite 6.13.7.2 Security Update (Important) (RHSA-2024:6337)]	critical
9/4/2024	[RHEL 8 : Satellite 6.15.3.1 Security Update (Important) (RHSA-2024:6335)]	critical
9/4/2024	[RHEL 8 : Satellite 6.14.4.2 Security Update (Important) (RHSA-2024:6336)]	critical
9/4/2024	[AlmaLinux 9 : wget (ALSA-2024:6192)]	critical
9/4/2024	[AlmaLinux 9 : krb5 (ALSA-2024:6166)]	critical
9/4/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : openssl-3 (SUSE-SU-2024:3105-1)]	high
9/4/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : xen (SUSE-SU-2024:3113-1)]	high
9/4/2024	[SUSE SLES15 Security Update : frr (SUSE-SU-2024:3090-1)]	high
9/4/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : openssl-3 (SUSE-SU-2024:3106-1)]	high
9/4/2024	[SUSE SLES15 Security Update : openssl-3 (SUSE-SU-2024:3107-1)]	high
9/4/2024	[SUSE SLES15 / openSUSE 15 Security Update : kubernetes1.28 (SUSE-SU-2024:3097-1)]	high

Datum	Schwachstelle	Bewertung
9/4/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : ucode-intel (SUSE-SU-2024:3095-1)]	high
9/4/2024	[SUSE SLES15 / openSUSE 15 Security Update : frr (SUSE-SU-2024:3108-1)]	high
9/4/2024	[SUSE SLES15 / openSUSE 15 Security Update : kubernetes1.27 (SUSE-SU-2024:3098-1)]	high
9/4/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : tiff (SUSE-SU-2024:3117-1)]	high
9/4/2024	[Oracle Linux 9 : postgresql (ELSA-2024-5999)]	high
9/4/2024	[Photon OS 5.0: Linux PHSA-2024-5.0-0360]	high
9/4/2024	[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Twisted vulnerabilities (USN-6988-1)]	high
9/4/2024	[RHEL 8 : kernel (RHSA-2024:6297)]	high
9/4/2024	[Google Chrome < 128.0.6613.120 Multiple Vulnerabilities]	high
9/4/2024	[Google Chrome < 128.0.6613.119 Multiple Vulnerabilities]	high
9/4/2024	[Google Chrome < 128.0.6613.119 Multiple Vulnerabilities]	high
9/4/2024	[RHEL 8 : resource-agents (RHSA-2024:6311)]	high
9/4/2024	[RHEL 9 : kpatch-patch-5_14_0-284_52_1 and kpatch-patch-5_14_0-284_79_1 (RHSA-2024:6313)]	high
9/4/2024	[RHEL 8 : fence-agents (RHSA-2024:6309)]	high
9/4/2024	[RHEL 9 : python3.11-setuptools (RHSA-2024:6312)]	high
9/4/2024	[Ubuntu 14.04 LTS : ImageMagick vulnerabilities (USN-6985-1)]	high
9/4/2024	[OracleVM 3.4 : kernel-uek (OVMSA-2024-0011)]	high
9/4/2024	[Oracle Linux 8 : fence-agents (ELSA-2024-6309)]	high
9/4/2024	[SEH Computertechnik UTN Server PRO and INU-100 Stored Cross-Site Scripting (CVE-2024-5420)]	high
9/4/2024	[SEH Computertechnik UTN Server PRO and INU-100 OS Command Injection (CVE-2024-5421)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Wed, 04 Sep 2024

Linux Kernel 5.6.13 Use-After-Free

Proof of concept exploit that uses a use-after-free vulnerability due to a race condition in MIDI devices in Linux Kernel version 5.6.13.

- Link

—

” “Wed, 04 Sep 2024

Mali GPU Kernel Local Privilege Escalation

This article provides an in-depth analysis of two kernel vulnerabilities within the Mali GPU, reachable from the default application sandbox, which the researcher independently identified and reported to Google. It includes a kernel exploit that achieves arbitrary kernel r/w capabilities. Consequently, it disables SELinux and elevates privileges to root on Google Pixel 7 and 8 Pro models.

- Link

—

” “Wed, 04 Sep 2024

Backdoor.Win32.Symmi.qua MVID-2024-0692 Buffer Overflow

Backdoor.Win32.Symmi.qua malware suffers from a buffer overflow vulnerability.

- Link

—

” “Wed, 04 Sep 2024

HackTool.Win32.Freezer.br (WinSpy) MVID-2024-0691 Insecure Credential Storage

HackTool.Win32.Freezer.br (WinSpy) malware suffers from an insecure credential storage vulnerability.

- Link

—

” “Wed, 04 Sep 2024

Backdoor.Win32.Optix.02.b MVID-2024-0690 Hardcoded Credential

Backdoor.Win32.Optix.02.b malware suffers from a hardcoded credential vulnerability.

- Link

—

” “Wed, 04 Sep 2024

Backdoor.Win32.JustJoke.21 (BackDoor Pro - v2.0b4) MVID-2024-0689 Code Execution

Backdoor.Win32.JustJoke.21 (BackDoor Pro - v2.0b4) malware suffers from a code execution vulnerability.

- Link

—

” “Wed, 04 Sep 2024

Backdoor.Win32.PoisonIvy.ymw MVID-2024-0688 Insecure Credential Storage

Backdoor.Win32.PoisonIvy.ymw malware suffers from an insecure credential storage vulnerability.

- Link

—

” “Wed, 04 Sep 2024

Online Travel Agency System 1.0 Shell Upload

Online Travel Agency System version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Wed, 04 Sep 2024

Tourism Management System 1.0 SQL Injection

Tourism Management System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Wed, 04 Sep 2024

Tenant courier management 1.0 Insecure Settings

Tenant courier management version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Wed, 04 Sep 2024

Supply Chain Management 1.0 SQL Injection

Supply Chain Management version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Wed, 04 Sep 2024

Student Result Management System 2.0 Insecure Direct Object Reference

Student Result Management System version 2.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Wed, 04 Sep 2024

Student Record System 1.0 SQL Injection

Student Record System version 1.0 suffers from a remote SQL injection vulnerability that allows for

authentication bypass.

- Link

—

” “Wed, 04 Sep 2024

Student Attendance Management System 1.0 Arbitrary File Upload

Student Attendance Management System version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Wed, 04 Sep 2024

Online Course Registration 1.0 SQL Injection

Online Course Registration version 1.0 suffers from a remote blind SQL injection vulnerability.

- Link

—

” “Tue, 03 Sep 2024

Texas Instruments Fusion Digital Power Designer 7.10.1 Credential Disclosure

Texas Instruments Fusion Digital Power Designer version 7.10.1 allows a local attacker to obtain sensitive information via the plaintext storage of credentials.

- Link

—

” “Tue, 03 Sep 2024

Taskhub 2.8.8 Insecure Settings

Taskhub version 2.8.8 suffers from an ignored default credential vulnerability.

- Link

—

” “Tue, 03 Sep 2024

Webpay E-Commerce 1.0 SQL Injection

Webpay E-Commerce version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Tue, 03 Sep 2024

SPIP 4.2.9 Code Execution

SPIP version 4.2.9 suffers from a code execution vulnerability.

- Link

—

” “Tue, 03 Sep 2024

Online Traffic Offense 1.0 Cross Site Request Forgery

Online Traffic Offense version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Tue, 03 Sep 2024

Penglead 2.0 Cross Site Scripting

Penglead version 2.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Tue, 03 Sep 2024

PPDB 2.4-update 6118-1 Cross Site Request Forgery

PPDB version 2.4-update 6118-1 suffers from a cross site request forgery vulnerability.

- Link

—

” “Tue, 03 Sep 2024

Online Travel Agency System 1.0 Arbitrary File Upload

Online Travel Agency System version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Mon, 02 Sep 2024

Packet Storm New Exploits For August, 2024

This archive contains all of the 722 exploits added to Packet Storm in August, 2024. Please note the increase in size for this month is due to a massive backlog of older exploits being added to the archive and is not representative of an uptick in new issues being discovered.

- Link

—

” “Mon, 02 Sep 2024

IntelliNet 2.0 Remote Root

Zero day remote root exploit for IntelliNet version 2.0. It affects multiple devices of AES Corp and Siemens. The exploit provides a remote shell and escalates your permissions to full root permissions by abusing exec_suid. No authentication needed at all, neither any interaction from the victim. The firmware affected by this exploit runs on fire alarms, burglar sensors and environmental devices, all on the internet, all vulnerable, no patch. Full control over hardware and software with no restrictions, you can manipulate battery voltage and even damage the hardware with unknown outcomes.

- Link

—

”

4.2 0-Days der letzten 5 Tage

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 X-Correlation-Id: An der Flughafen-Security vorbei mit SQL-Injection.

Zum Youtube Video

6 Cyberangriffe: (Sep)

Datum	Opfer	Land	Information
2024-09-02	Transport for London (TfL)	[GBR]	Link
2024-09-02	Conseil national de l'ordre des experts-comptables (CNOEC)	[FRA]	Link
2024-09-01	Wertachkliniken	[DEU]	Link

7 Ransomware-Erpressungen: (Sep)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-05	[www.parknfly.ca]	ransomhub	Link
2024-09-05	[Western Supplies, Inc]	bianlian	Link
2024-09-04	[Farmers' Rice Cooperative]	play	Link
2024-09-04	[Bakersfield]	play	Link
2024-09-04	[Crain Group]	play	Link
2024-09-04	[Parrish]	blacksuit	Link
2024-09-04	[Seirus Innovation]	play	Link
2024-09-04	[www.galgorm.com]	ransomhub	Link
2024-09-04	[www.pcipa.com]	ransomhub	Link
2024-09-04	[OSDA Contract Services]	blacksuit	Link
2024-09-04	[ych.com]	madliberator	Link
2024-09-04	[www.bennettcurrie.co.nz]	ransomhub	Link
2024-09-03	[idom.com]	lynx	Link
2024-09-04	[plannedparenthood.org]	ransomhub	Link
2024-09-04	[Sunrise Erectors]	hunters	Link
2024-09-03	[gardenhomesmanagement.com]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-03	[simson-maxwell.com]	cactus	Link
2024-09-03	[balboabayresort.com]	cactus	Link
2024-09-03	[flodraulic.com]	cactus	Link
2024-09-03	[mcphillips.co.uk]	cactus	Link
2024-09-03	[rangeramerican.com]	cactus	Link
2024-09-03	[Turman]	qilin	Link
2024-09-02	[Kingsport Imaging Systems]	medusa	Link
2024-09-02	[www.amberbev.com]	ransomhub	Link
2024-09-02	[www.sanyo-bussan.co.jp]	ransomhub	Link
2024-09-02	[www.pokerspa.it]	ransomhub	Link
2024-09-02	[Removal.AI]	ransomhub	Link
2024-09-02	[Project Hospitality]	rhysida	Link
2024-09-02	[Shomof Group]	medusa	Link
2024-09-02	[www.sanyo-av.com]	ransomhub	Link
2024-09-02	[www.schneider.ch]	ransomhub	Link
2024-09-01	[Quálitas México]	hunters	Link
2024-09-01	[welland]	trinity	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.