Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240907

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

WordPress-Plug-in LiteSpeed Cache erneut angreifbar

Mehr als 6 Millionen WordPress-Websites setzen das Plug-in LiteSpeed Cache ein. Nun wurde abermals eine Sicherheitslücke geschlossen.

- Link

—

Apache OFBiz: Aktueller Sicherheitspatch repariert ältere Patches

Ein aktueller Patch für Apache OFBiz verhindert, dass Sicherheitsupdates für ältere Lücken umgangen werden können.

- Link

—

Veeam behebt mehrere Sicherheitslücken - Codeschmuggel möglich

Angreifer konnten eigenen zudem Dateien aus der Ferne löschen, die Authentifizierung manipulieren und ihre Privilegien erhöhen. Patches stehen bereit.

- Link

—

Angreifer können durch Hintertür in Cisco Smart Licensing Utility schlüpfen

Es sind wichtige Sicherheitsupdates für mehrere Produkte des Netzwerkausrüster Cisco erschienen.

- Link

—

Zyxel: Angreifer können Kontrolle über Access Points und Router erlangen

Ein Sicherheitsupdate schließt eine kritische Sicherheitslücke unter anderem in Access-Point-Modellen von Zyxel.

- Link

—

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
—

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	0.994760000	Link
CVE-2023-6895	0.921160000	0.990170000	Link
CVE-2023-6553	0.937150000	0.991810000	Link
CVE-2023-6019	0.918710000	0.989910000	Link
CVE-2023-5360	0.902780000	0.988870000	Link
CVE-2023-52251	0.946410000	0.992930000	Link
CVE-2023-4966	0.970940000	0.998180000	Link
CVE-2023-49103	0.949680000	0.993470000	Link
CVE-2023-48795	0.965330000	0.996460000	Link
CVE-2023-47246	0.956040000	0.994590000	Link
CVE-2023-46805	0.950230000	0.993570000	Link
CVE-2023-46747	0.972260000	0.998650000	Link
CVE-2023-46604	0.968800000	0.997420000	Link
CVE-2023-4542	0.948590000	0.993290000	Link
CVE-2023-43208	0.973970000	0.999380000	Link
CVE-2023-43177	0.961750000	0.995560000	Link
CVE-2023-42793	0.971190000	0.998310000	Link
CVE-2023-41265	0.907590000	0.989180000	Link
CVE-2023-39143	0.936490000	0.991750000	Link
CVE-2023-38205	0.953670000	0.994170000	Link
CVE-2023-38203	0.965830000	0.996600000	Link
CVE-2023-38146	0.920720000	0.990110000	Link
CVE-2023-38035	0.974690000	0.999720000	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	0.997970000	Link
CVE-2023-34993	0.973540000	0.999190000	Link
CVE-2023-34960	0.921610000	0.990230000	Link
CVE-2023-34634	0.923140000	0.990370000	Link
CVE-2023-34362	0.970450000	0.997970000	Link
CVE-2023-34039	0.947070000	0.993040000	Link
CVE-2023-3368	0.942130000	0.992350000	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	0.997570000	Link
CVE-2023-29298	0.969880000	0.997760000	Link
CVE-2023-28432	0.907350000	0.989160000	Link
CVE-2023-28343	0.933130000	0.991440000	Link
CVE-2023-28121	0.919520000	0.989990000	Link
CVE-2023-27524	0.970600000	0.998020000	Link
CVE-2023-27372	0.973470000	0.999170000	Link
CVE-2023-27350	0.968480000	0.997320000	Link
CVE-2023-26469	0.953890000	0.994210000	Link
CVE-2023-26360	0.964390000	0.996160000	Link
CVE-2023-26035	0.969020000	0.997470000	Link
CVE-2023-25717	0.954660000	0.994330000	Link
CVE-2023-25194	0.966980000	0.996930000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963960000	0.996050000	Link
CVE-2023-24489	0.973820000	0.999320000	Link
CVE-2023-23752	0.956380000	0.994640000	Link
CVE-2023-23333	0.961070000	0.995420000	Link
CVE-2023-22527	0.970940000	0.998190000	Link
CVE-2023-22518	0.961800000	0.995570000	Link
CVE-2023-22515	0.972760000	0.998890000	Link
CVE-2023-21839	0.955020000	0.994400000	Link
CVE-2023-21554	0.955880000	0.994560000	Link
CVE-2023-20887	0.970840000	0.998130000	Link
CVE-2023-1671	0.962690000	0.995730000	Link
CVE-2023-0669	0.971330000	0.998380000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 06 Sep 2024

[UPDATE] [hoch] libarchive: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Fri, 06 Sep 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Fri, 06 Sep 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, 06 Sep 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, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen oder Cross-Site-Scripting (XSS)-Angriffe durchzuführen.

- Link

—

Fri, 06 Sep 2024

[UPDATE] [hoch] Red Hat Ansible Automation Platform: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat Ansible Automation Platform ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand erzeugen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder Cross-Site-Scripting (XSS)-Angriffe durchzuführen.

- Link

—

Fri, 06 Sep 2024

[UPDATE] [hoch] Microsoft Azure: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein Angreifer kann mehrere Schwachstellen in Microsoft Azure ausnutzen, um seine Privilegien zu erhöhen und um einen Denial of Service Zustand herbeizuführen.

- Link

—

Fri, 06 Sep 2024

[UPDATE] [hoch] Mozilla Firefox: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Firefox ESR ausnutzen, um beliebigen Code auszuführen, um einen Denial of Service Zustand herbeizuführen und um Sicherheitsmechanismen zu umgehen, sowie den Benutzer zu täuschen.

- Link

—

Fri, 06 Sep 2024

[UPDATE] [hoch] Red Hat OpenShift: Schwachstelle ermöglicht Denial of Service

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

- Link

—

Fri, 06 Sep 2024

[UPDATE] [hoch] IBM WebSphere Application Server: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in IBM WebSphere Application Server ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Fri, 06 Sep 2024

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

Ein entfernter, anonymer 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, 06 Sep 2024

[UPDATE] [kritisch] Microsoft Windows: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in verschiedenen Versionen von Microsoft Windows und Microsoft Windows Server ausnutzen, um seine Privilegien zu erweitern, beliebigen Programmcode auszuführen, Informationen offenzulegen, Dateien zu manipulieren oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Fri, 06 Sep 2024

[UPDATE] [hoch] Django: Mehrere Schwachstellen

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

- Link

—

Fri, 06 Sep 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

—

Fri, 06 Sep 2024

[UPDATE] [hoch] Oracle Communications: Mehrere Schwachstellen

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Oracle Communications ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.
- Link

—

Fri, 06 Sep 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, 06 Sep 2024

[UPDATE] [hoch] docker: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in docker ausnutzen, um seine Privilegien zu erhöhen.
- Link

—

Fri, 06 Sep 2024

[UPDATE] [hoch] Red Hat Enterprise Linux (python-setuptools): Schwachstelle ermöglicht Code-ausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Fri, 06 Sep 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

—

Fri, 06 Sep 2024

[UPDATE] [hoch] IBM QRadar SIEM: Mehrere Schwachstellen

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in IBM QRadar SIEM ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, Daten zu manipulieren, vertrauliche Informationen offenzulegen, eine Man-in-the-Middle-Situation zu schaffen, Sicherheits-maßnahmen zu umgehen oder eine Denial-of-Service-Situation zu schaffen.
- Link

—

Fri, 06 Sep 2024

[UPDATE] [hoch] SonicWall SonicOS: Schwachstelle ermöglicht Offenlegung von Informationen und Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in SonicWall SonicOS ausnutzen, um Informationen offenzulegen und um einen Denial of Service Angriff durchzuführen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/6/2024	[FreeBSD : FreeBSD – umtx Kernel panic or Use-After-Free (7e079ce2-6b51-11ef-9a62-002590c1f29c)]	critical
9/6/2024	[FreeBSD : firefox – multiple vulnerabilities (a3a1caf5-6ba1-11ef-b9e8-b42e991fc52e)]	critical
9/6/2024	[Photon OS 3.0: Krb5 PHSA-2024-3.0-0791]	critical
9/6/2024	[Fedora 39 : python3.11 (2024-dab2a69be9)]	critical
9/6/2024	[Fedora 39 : python3.9 (2024-dc7f1d57e4)]	critical
9/6/2024	[Fedora 39 : python3.13 (2024-992047a33f)]	critical
9/6/2024	[Veeam Backup and Replication 12.x < 12.2.0.334 Multiple Vulnerabilities (September 2024) (KB4649)]	critical
9/6/2024	[AlmaLinux 8 : bubblewrap and flatpak (ALSA-2024:6422)]	critical
9/6/2024	[Photon OS 5.0: Krb5 PHSA-2024-5.0-0355]	critical
9/6/2024	[Photon OS 5.0: Libxml2 PHSA-2024-5.0-0354]	critical
9/6/2024	[Photon OS 4.0: Krb5 PHSA-2024-4.0-0679]	critical
9/6/2024	[Mozilla Thunderbird < 115.15]	critical
9/6/2024	[Mozilla Thunderbird < 115.15]	critical
9/6/2024	[Mozilla Thunderbird < 128.2]	critical

Datum	Schwachstelle	Bewertung
9/6/2024	[Mozilla Thunderbird < 128.2]	critical
9/6/2024	[F5 Networks BIG-IP : libarchive vulnerability (K000140963)]	high
9/6/2024	[F5 Networks BIG-IP : libarchive vulnerability (K000140961)]	high
9/6/2024	[SUSE SLES15 Security Update : hdf5, netcdf, trilinos (SUSE-SU-2024:3144-1)]	high
9/6/2024	[openSUSE 15 Security Update : chromium (openSUSE-SU-2024:0278-1)]	high
9/6/2024	[Fedora 40 : python-django4.2 (2024-865828665c)]	high
9/6/2024	[Fedora 40 : mingw-python3 (2024-3d656dafe1)]	high
9/6/2024	[Fedora 39 : lua-mpack (2024-a84c59eedc)]	high
9/6/2024	[Fedora 40 : python-django (2024-4a08381122)]	high
9/6/2024	[Fedora 40 : lua-mpack (2024-430678b035)]	high
9/6/2024	[Fedora 39 : python-django4.2 (2024-28892f7c8f)]	high
9/6/2024	[Fedora 39 : mingw-python3 (2024-7008b2fedf)]	high
9/6/2024	[Fedora 39 : python-django (2024-e2bde0853b)]	high
9/6/2024	[ManageEngine Endpoint Central < 11.3.2400.15 , < 11.3.2406.08 Incorrect Authorization vulnerability]	high
9/6/2024	[Tenable Security Center Multiple Vulnerabilities (TNS-2024-12)]	high
9/6/2024	[Nutanix AOS : Multiple Vulnerabilities (NXSA-AOS-6.8.1.5)]	high
9/6/2024	[Photon OS 4.0: Linux PHSA-2024-4.0-0678]	high
9/6/2024	[Photon OS 5.0: Unbound PHSA-2024-5.0-0357]	high
9/6/2024	[Photon OS 4.0: Python3 PHSA-2024-4.0-0673]	high
9/6/2024	[Photon OS 4.0: Linux PHSA-2024-4.0-0677]	high
9/6/2024	[Photon OS 5.0: Linux PHSA-2024-5.0-0359]	high
9/6/2024	[Photon OS 4.0: Unbound PHSA-2024-4.0-0677]	high
9/6/2024	[Zyxel USG 4.60 < 5.39 / ATP 4.60 < 5.39 Command Injection]	high
9/6/2024	[Zyxel USG FLEX 4.50 < 5.39 / ATP 4.32 < 5.39 Multiple Vulnerabilities]	high

Datum	Schwachstelle	Bewertung
9/6/2024	[Zyxel USG FLEX 5.00 < 5.39 / ATP 5.00 < 5.39 Command Injection]	high
9/6/2024	[Zyxel USG FLEX 4.16 < 5.39 Multiple Vulnerabilities]	high
9/6/2024	[Zyxel USG FLEX 4.20 < 5.39 DoS]	high
9/6/2024	[ABB Freelance AC 900F and AC 700F Stack-based Buffer Overflow (CVE-2023-0426)]	high
9/6/2024	[ABB Freelance AC 900F and AC 700F Numeric Range Comparison Without Minimum Check (CVE-2023-0425)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Fri, 06 Sep 2024

C-MOR Video Surveillance 5.2401 / 6.00PL01 Command Injection

C-MOR Video Surveillance versions 5.2401 and 6.00PL01 suffer from a command injection vulnerability.

- Link

—

” “Fri, 06 Sep 2024

C-MOR Video Surveillance 5.2401 / 6.00PL01 Information Disclosure / Cleartext Secret

C-MOR Video Surveillance versions 5.2401 and 6.00PL01 stores sensitive information, such as credentials, in clear text.

- Link

—

” “Fri, 06 Sep 2024

C-MOR Video Surveillance 5.2401 / 6.00PL01 Privilege Escalation

C-MOR Video Surveillance versions 5.2401 and 6.00PL01 suffer from an improper privilege management vulnerability that can allows for privilege escalation.

- Link

—

” “Fri, 06 Sep 2024

C-MOR Video Surveillance 5.2401 Remote Shell Upload

C-MOR Video Surveillance version 5.2401 suffers from a remote shell upload vulnerability.
- Link

—

” “Fri, 06 Sep 2024

C-MOR Video Surveillance 5.2401 Path Traversal

C-MOR Video Surveillance version 5.2401 suffers from a path traversal vulnerability.
- Link

—

” “Fri, 06 Sep 2024

C-MOR Video Surveillance 5.2401 Improper Access Control

C-MOR Video Surveillance version 5.2401 suffers from an improper access control privilege escalation vulnerability that allows for a lower privileged user to access administrative functions.
- Link

—

” “Fri, 06 Sep 2024

C-MOR Video Surveillance 5.2401 / 6.00PL01 SQL Injection

C-MOR Video Surveillance versions 5.2401 and 6.00PL01 suffer from a remote SQL injection vulnerability.
- Link

—

” “Fri, 06 Sep 2024

C-MOR Video Surveillance 5.2401 / 6.00PL01 Cross Site Request Forgery

C-MOR Video Surveillance versions 5.2401 and 6.00PL01 suffer from a cross site request forgery vulnerability.
- Link

—

” “Fri, 06 Sep 2024

C-MOR Video Surveillance 5.2401 / 6.00PL01 Cross Site Scripting

C-MOR Video Surveillance versions 5.2401 and 6.00PL01 suffer from a persistent cross site scripting vulnerability.
- Link

—

” “Fri, 06 Sep 2024

C-MOR Video Surveillance 5.2401 Cross Site Scripting

C-MOR Video Surveillance version 5.2401 suffers from a reflective cross site scripting vulnerability.
- Link

—

” “Fri, 06 Sep 2024

Travel 1.0 Shell Upload

Travel version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Fri, 06 Sep 2024

Webpay E-Commerce 1.0 Insecure Settings

Webpay E-Commerce version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Fri, 06 Sep 2024

SPIP 4.2.12 Code Execution

SPIP version 4.2.12 suffers from a code execution vulnerability.

- Link

—

” “Fri, 06 Sep 2024

Online Sports Complex Booking System 1.0 Insecure Settings

Online Sports Complex Booking System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Fri, 06 Sep 2024

Online Shopping Portal Project 2.0 SQL Injection

Online Shopping Portal Project version 2.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Fri, 06 Sep 2024

Online Pizza Ordering System 1.0 Insecure Settings

Online Pizza Ordering System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Fri, 06 Sep 2024

File Management System 1.0 Insecure Direct Object Reference

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

- Link

—

” “Fri, 06 Sep 2024

Crime Complaints Reporting Management System 1.0 Arbitrary File Upload

Crime Complaints Reporting Management System version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Fri, 06 Sep 2024

Blood Bank And Donor Management System 2.4 Insecure Settings

Blood Bank and Donor Management System version 2.4 suffers from an ignored default credential vulnerability.

- Link

—

” “Thu, 05 Sep 2024

ASUS RT-AC3200 3.0.0.4.382.50010 Command Injection

Proof of concept exploit demonstrating a remote command injection vulnerability in ASUS RT-AC3200 version 3.0.0.4.382.50010.

- Link

—

” “Thu, 05 Sep 2024

ASIS 3.2.0 SQL Injection

Aplikasi Sistem Sekolah using CodeIgniter 3 versions 3.0.0 through 3.2.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “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
—
”

4.2 0-Days der letzten 5 Tage

“Thu, 05 Sep 2024
ZDI-24-1195: Malwarebytes Antimalware Link Following Local Privilege Escalation Vulnerability
- Link
—
” “Thu, 05 Sep 2024
ZDI-24-1194: Linux Kernel Plan 9 File System Race Condition Local Privilege Escalation Vulnerability
- Link
—
” “Thu, 05 Sep 2024
ZDI-24-1193: Delta Electronics DIAScreen DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability
- Link
—
”

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
2024-09-05	Air-e	[COL]	Link
2024-09-04	Tewkesbury Borough Council	[GBR]	Link
2024-09-04	Swire Pacific Offshore (SPO)	[SGP]	Link
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	[briedis.lt]	ransomhub	Link
2024-09-06	[America Voice]	medusa	Link
2024-09-06	[CK Associates]	bianlian	Link
2024-09-06	[Keya Accounting and Tax Services LLC]	bianlian	Link
2024-09-06	[ctelift.com]	madliberator	Link
2024-09-06	[SESAM Informatics]	hunters	Link
2024-09-06	[riomarineinc.com]	cactus	Link
2024-09-06	[champeau.com]	cactus	Link
2024-09-05	[cda.be]	killsec	Link
2024-09-05	[belfius.be]	killsec	Link
2024-09-05	[dvv.be]	killsec	Link
2024-09-05	[Custom Security Systems]	hunters	Link
2024-09-05	[Inglenorth.co.uk]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-05	[cps-k12.org]	ransomhub	Link
2024-09-05	[inorde.com]	ransomhub	Link
2024-09-05	[tri-tech.us]	ransomhub	Link
2024-09-05	[PhD Services]	dragonforce	Link
2024-09-05	[kawasaki.eu]	ransomhub	Link
2024-09-05	[phdservices.net]	ransomhub	Link
2024-09-05	[cbt-gmbh.de]	ransomhub	Link
2024-09-05	[www.towellengineering.net]	ransomhub	Link
2024-09-04	[rhp.com.br]	lockbit3	Link
2024-09-05	[Baird Mandalas Brockstedt LLC]	akira	Link
2024-09-05	[Imetame]	akira	Link
2024-09-05	[SWISS CZ]	akira	Link
2024-09-05	[Cellular Plus]	akira	Link
2024-09-05	[Arch Street Capital Advisors]	qilin	Link
2024-09-04	[Hospital Episcopal San Lucas]	medusa	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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.