Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240910

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

Loadbalancer: Angreifer können LoadMaster kompromittieren

Es sind wichtige Sicherheitspatches für LoadMaster und MultiTenant Hypervisor von Progress Kemp erschienen.

- Link

—

Schadcode-Lücken gefährden Visualiserungsplattform Kibana

Ein Sicherheitsupdate schließt zwei kritische Sicherheitslücken in Kibana.

- Link

—

Jetzt patchen! Angreifer attackieren Firewalls von Sonicwall

Mittlerweile ist klar, dass eine Schwachstelle nicht nur SonicOS, sondern auch die SSLVPN-Funktion betrifft. Sicherheitsupdates sind verfügbar.

- Link

—

Qnap: Zahlreiche Updates für mehrere Produkte

Qnap hat eine Reihe von Softwareaktualisierungen veröffentlicht, die Schwachstellen in mehreren Produkten ausbessern.

- Link

—

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

—

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	0.994770000	Link
CVE-2023-6895	0.921160000	0.990180000	Link
CVE-2023-6553	0.937150000	0.991820000	Link
CVE-2023-6019	0.918710000	0.989920000	Link
CVE-2023-5360	0.902780000	0.988870000	Link
CVE-2023-52251	0.946410000	0.992950000	Link
CVE-2023-4966	0.970840000	0.998130000	Link
CVE-2023-49103	0.949680000	0.993500000	Link
CVE-2023-48795	0.965330000	0.996460000	Link
CVE-2023-47246	0.956040000	0.994600000	Link
CVE-2023-46805	0.950230000	0.993590000	Link
CVE-2023-46747	0.972260000	0.998650000	Link
CVE-2023-46604	0.968800000	0.997440000	Link
CVE-2023-4542	0.948590000	0.993320000	Link
CVE-2023-43208	0.973970000	0.999380000	Link
CVE-2023-43177	0.961750000	0.995580000	Link
CVE-2023-42793	0.971190000	0.998300000	Link
CVE-2023-41265	0.907590000	0.989180000	Link
CVE-2023-39143	0.936490000	0.991760000	Link
CVE-2023-38205	0.950330000	0.993600000	Link
CVE-2023-38203	0.965830000	0.996610000	Link
CVE-2023-38146	0.920720000	0.990120000	Link
CVE-2023-38035	0.974690000	0.999720000	Link
CVE-2023-36845	0.966750000	0.996870000	Link
CVE-2023-3519	0.965910000	0.996630000	Link
CVE-2023-35082	0.967460000	0.997060000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-35078	0.970930000	0.998180000	Link
CVE-2023-34993	0.973450000	0.999170000	Link
CVE-2023-34960	0.921610000	0.990240000	Link
CVE-2023-34634	0.923140000	0.990380000	Link
CVE-2023-34362	0.970450000	0.997970000	Link
CVE-2023-34039	0.947070000	0.993060000	Link
CVE-2023-3368	0.942130000	0.992360000	Link
CVE-2023-33246	0.967180000	0.996970000	Link
CVE-2023-32315	0.970220000	0.997880000	Link
CVE-2023-30625	0.953610000	0.994170000	Link
CVE-2023-30013	0.965950000	0.996640000	Link
CVE-2023-29300	0.969240000	0.997580000	Link
CVE-2023-29298	0.970810000	0.998100000	Link
CVE-2023-28432	0.907350000	0.989160000	Link
CVE-2023-28343	0.933130000	0.991440000	Link
CVE-2023-28121	0.925430000	0.990620000	Link
CVE-2023-27524	0.970600000	0.998010000	Link
CVE-2023-27372	0.973930000	0.999350000	Link
CVE-2023-27350	0.968480000	0.997330000	Link
CVE-2023-26469	0.953890000	0.994230000	Link
CVE-2023-26360	0.964390000	0.996160000	Link
CVE-2023-26035	0.968440000	0.997320000	Link
CVE-2023-25717	0.954660000	0.994350000	Link
CVE-2023-25194	0.966980000	0.996930000	Link
CVE-2023-2479	0.963960000	0.996060000	Link
CVE-2023-24489	0.973820000	0.999320000	Link
CVE-2023-23752	0.951460000	0.993780000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23333	0.961070000	0.995440000	Link
CVE-2023-22527	0.970940000	0.998190000	Link
CVE-2023-22518	0.961800000	0.995580000	Link
CVE-2023-22515	0.972760000	0.998900000	Link
CVE-2023-21839	0.951270000	0.993720000	Link
CVE-2023-21554	0.955880000	0.994570000	Link
CVE-2023-20887	0.970840000	0.998120000	Link
CVE-2023-1671	0.962690000	0.995740000	Link
CVE-2023-0669	0.971330000	0.998380000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 09 Sep 2024

[NEU] [hoch] QNAP NAS QTS and QuTS hero: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in QNAP NAS ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmaßnahmen zu umgehen und erweiterte Rechte zu erlangen.

- Link

—

Mon, 09 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

—

Mon, 09 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 oder Daten zu manipulieren.

- Link

—

Mon, 09 Sep 2024

[NEU] [hoch] Synology Router Manager: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Synology Router Manager ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 09 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

—

Mon, 09 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

—

Mon, 09 Sep 2024

[UPDATE] [hoch] Ghostscript: Mehrere Schwachstellen

Ein entfernter anonymer oder ein lokaler Angreifer kann mehrere Schwachstellen in Ghostscript ausnutzen, um Informationen offenzulegen oder beliebigen Code auszuführen.

- Link

—

Mon, 09 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

—

Mon, 09 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

—

Mon, 09 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

—

Mon, 09 Sep 2024

[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Code auszuführen oder einen unspezifischen Angriff durchzuführen.

- Link

—

Mon, 09 Sep 2024

[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Code auszuführen oder einen unspezifischen Angriff durchzuführen.

- Link

—

Mon, 09 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

—

Mon, 09 Sep 2024

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

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

- Link

—

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

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/9/2024	[Debian dla-3882 : thunderbird - security update]	critical
9/9/2024	[RHEL 8 / 9 : Red Hat Ansible Automation Platform 2.4 Product Security and Bug Fix Update (Moderate) (RHSA-2024:6428)]	critical
9/9/2024	[RHEL 8 : bubblewrap and flatpak (RHSA-2024:6421)]	critical
9/9/2024	[Nutanix AHV : (NXSA-AHV-20220304.392)]	critical
9/9/2024	[SonicWall SonicOS Improper Access Control (SNWLID-2024-0015)]	critical
9/9/2024	[RHEL 9 : emacs (RHSA-2024:6510)]	critical
9/9/2024	[Oracle Linux 9 : emacs (ELSA-2024-6510)]	critical
9/9/2024	[Amazon Linux 2023 : runc (ALAS2023-2024-710)]	critical
9/9/2024	[Amazon Linux 2023 : docker (ALAS2023-2024-711)]	critical
9/9/2024	[Amazon Linux 2 : thunderbird (ALAS-2024-2629)]	critical
9/9/2024	[F5 Networks BIG-IP : RADIUS authentication vulnerability (K000141008)]	critical
9/9/2024	[Nexans FTTO GigaSwitch Backdoor Account (CVE-2022-32985)]	critical
9/9/2024	[Citrix Workspace App for Windows Privilege Escalation (CTX678036)]	high
9/9/2024	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : LibTIFF vulnerability (USN-6997-1)]	high
9/9/2024	[Slackware Linux 15.0 / current netatalk Multiple Vulnerabilities (SSA:2024-253-01)]	high
9/9/2024	[Nutanix AHV : Multiple Vulnerabilities (NXSA-AHV-20220304.441)]	high

Datum	Schwachstelle	Bewertung
9/9/2024	[Nutanix AHV : Multiple Vulnerabilities (NXSA-AHV-20220304.423)]	high
9/9/2024	[Atlassian Confluence < 7.19.26 / 7.20.x < 8.5.14 / 8.6.x < 9.0.1 (CONFSERVER-97720)]	high
9/9/2024	[RHEL 8 : Red Hat Single Sign-On 7.6.10 security update on RHEL 8 (Moderate) (RHSA-2024:6494)]	high
9/9/2024	[RHEL 7 : Red Hat Single Sign-On 7.6.10 security update on RHEL 7 (Moderate) (RHSA-2024:6493)]	high
9/9/2024	[RHEL 9 : Red Hat Single Sign-On 7.6.10 security update on RHEL 9 (Moderate) (RHSA-2024:6495)]	high
9/9/2024	[Amazon Linux 2023 : bpftool, kernel, kernel-devel (ALAS2023-2024-709)]	high
9/9/2024	[Nutanix AHV : Multiple Vulnerabilities (NXSA-AHV-20230302.100173)]	high
9/9/2024	[Nutanix AHV : Multiple Vulnerabilities (NXSA-AHV-20230302.101026)]	high
9/9/2024	[Nutanix AHV : Multiple Vulnerabilities (NXSA-AHV-20230302.2008)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Mon, 09 Sep 2024

Microsoft Windows DWM Core Library Privilege Escalation

Proof of concept code for the Microsoft Windows DWM Core library elevation of privilege vulnerability. The researcher shows how they reversed the patch, how the heap overflow is produced, and overall gives a complete walk through of their process.

- Link

—

” “Mon, 09 Sep 2024

Breaking Oracle Database VPD Through DDL Permissions In 19c

By having specific DDL permissions set in Oracle 19c, you can bypass access restrictions normally in place for VPD (virtual private database).

- Link

—

” “Mon, 09 Sep 2024

PPDB 2.4-update 6118-1 SQL Injection

PPDB version 2.4-update 6118-1 suffers from a remote blind SQL injection vulnerability.

- Link

—

” “Mon, 09 Sep 2024

POMS 1.0 Insecure Settings

POMS version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 09 Sep 2024

Pharmacy Management System version 1.0 Insecure Settings

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

- Link

—

” “Mon, 09 Sep 2024

PDF Generator Web Application 1.0 Insecure Settings

PDF Generator Web Application version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 09 Sep 2024

Park Ticketing Project 1.0 SQL Injection

Park Ticketing Project version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Mon, 09 Sep 2024

Online Travel Agency System 1.0 Insecure Settings

Online Travel Agency System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 09 Sep 2024

Online Tours and Travels Management System 1.0 Insecure Settings

Online Tours and Travels Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 09 Sep 2024

Online Survey System 1.0 SQL Injection

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

- Link

—

” “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

—

”

4.2 0-Days der letzten 5 Tage

“Mon, 09 Sep 2024

ZDI-24-1196: Adobe Acrobat Reader DC Doc Object Use-After-Free Information Disclosure 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
2024-09-08	Highline Public Schools	[USA]	Link
2024-09-06	Superior Tribunal de Justiça (STJ)	[BRA]	Link
2024-09-05	Air-e	[COL]	Link
2024-09-05	Charles Darwin School	[GBR]	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
2024-09-06	[americagraphics.com]	ransomhub	Link
2024-09-09	[Pennsylvania State Education Association]	rhysida	Link
2024-09-09	[Anniversary Holding]	bianlian	Link
2024-09-09	[Battle Lumber Co.]	bianlian	Link
2024-09-09	[www.unige.it]	ransomhub	Link
2024-09-09	[www.dpe.go.th]	ransomhub	Link
2024-09-09	[www.bsg.com.au]	ransomhub	Link
2024-09-09	[www.avf-biomedical.com]	ransomhub	Link
2024-09-09	[schynsassurances.be]	killsec	Link
2024-09-09	[pv.be]	killsec	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-09	[Smart Source, Inc.]	bianlian	Link
2024-09-08	[CAM Tyre Trade Systems & Solutions]	qilin	Link
2024-09-09	[▒▒▒▒▒▒▒▒]	cicada3301	Link
2024-09-08	[Stratford School Academy]	rhysida	Link
2024-09-07	[cardiovirginia.com]	ransomhub	Link
2024-09-07	[Prosolit]	medusa	Link
2024-09-07	[Grupo Cortefiel]	medusa	Link
2024-09-07	[Nocciole Marchisio]	meow	Link
2024-09-07	[Elsoms Seeds]	meow	Link
2024-09-07	[Millsboro Animal Hospital]	qilin	Link
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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
2024-09-02	[Kingsport Imaging Systems]	medusa	Link
2024-09-02	[www.amberbev.com]	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
2024-09-01	[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.