Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240702

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

RegreSSHion: Sicherheitslücke in OpenSSH gibt geduldigen Angreifern Root-Rechte

Wer die alte, neue Lücke im SSH-Server ausnutzen möchte, braucht Sitzfleisch: Bis zur Root-Shell dauert es 8 Stunden. Dafür klappt der Angriff aus der Ferne.

- Link

—

IP-Telefonie: Avaya IP Office stopft kritische Sicherheitslecks

Updates für Avaya IP Office dichten Sicherheitslecks in der Software ab. Angreifer können dadurch Schadcode einschleusen.

- Link

—

Juniper: Kritische Lücke erlaubt Angreifern Übernahme von Session Smart Router

Juniper Networks liefert außerplanmäßige Updates gegen eine kritische Sicherheitslücke in Session Smart Router, -Conductor und WAN Assurance Router.

- Link

—

APT-Angriff auf Fernwartungssoftware? Sicherheitsvorfall bei TeamViewer

Noch ist über das Ausmaß des Angriffs gegen die Fernwartungssoftware nicht viel bekannt - erste Hinweise auf die Urheber deuten auf Profis hin.

- Link

—

Bitte patchen! Security-Update behebt kritische Schwachstelle in GitLab

Eine Reihe von Schwachstellen ermöglichen es in GitLab, CI-Pipelines als anderer User zu starten oder Cross-Site-Scripting über Commit Notes einzuschleusen.

- Link

—

Google Quickshare: Sicherheitslücke ermöglicht ungefragtes Senden von Dateien

Googles Quickshare, auch als Nearby Share bekannt, kann Angreifern ungefragt Daten an Windows-Rechner schicken lassen.

- Link

—

JavaScript-Service Polyfill.io: 100.000 Sites binden Schadcode über CDN ein

Mehrere Sicherheitsforscher melden eine aktive Bedrohung durch das Content Delivery Network von Polyfill.io. Google sperrt Werbung von betroffenen Ads-Seiten.

- Link

—

Jetzt patchen! Progress-MOVEit-Sicherheitslücken werden bereits angegriffen

Progress hat zwei kritische Lücken in MOVEit Gateway und Transfer gestopft. Eine davon attackieren Cyberkriminelle bereits.

- Link

—

Wordpress: Fünf Plug-ins mit Malware unterwandert

In fünf Wordpress-Plug-ins haben IT-Sicherheitsforscher dieselbe eingeschleuste Malware entdeckt. Nur für eines gibt es ein Update.

- Link

—

Juniper: 225 Sicherheitslücken in Secure Analytics

Juniper Networks hat eine Aktualisierung für Secure Analytics herausgegeben. Sie stopft 225 Sicherheitslecks, einige davon gelten als kritisch.

- 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	0.960230000	0.994970000	Link
CVE-2023-6895	0.920390000	0.989570000	Link
CVE-2023-6553	0.934680000	0.991130000	Link
CVE-2023-5360	0.911260000	0.988840000	Link
CVE-2023-52251	0.920390000	0.989580000	Link
CVE-2023-4966	0.971290000	0.998060000	Link
CVE-2023-49103	0.938900000	0.991620000	Link
CVE-2023-48795	0.962520000	0.995430000	Link
CVE-2023-47246	0.953220000	0.993740000	Link
CVE-2023-46805	0.958670000	0.994660000	Link
CVE-2023-46747	0.972100000	0.998370000	Link
CVE-2023-46604	0.963890000	0.995790000	Link
CVE-2023-4542	0.924200000	0.990000000	Link
CVE-2023-43208	0.956050000	0.994240000	Link
CVE-2023-43177	0.959300000	0.994810000	Link
CVE-2023-42793	0.970430000	0.997700000	Link
CVE-2023-41265	0.920320000	0.989560000	Link
CVE-2023-39143	0.944760000	0.992370000	Link
CVE-2023-38205	0.954590000	0.993980000	Link
CVE-2023-38203	0.968820000	0.997200000	Link
CVE-2023-38146	0.905210000	0.988430000	Link
CVE-2023-38035	0.974610000	0.999600000	Link
CVE-2023-36845	0.965980000	0.996350000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3519	0.965360000	0.996190000	Link
CVE-2023-35082	0.967870000	0.996920000	Link
CVE-2023-35078	0.968330000	0.997080000	Link
CVE-2023-34993	0.971260000	0.998050000	Link
CVE-2023-34960	0.927460000	0.990310000	Link
CVE-2023-34634	0.927960000	0.990340000	Link
CVE-2023-34468	0.906650000	0.988530000	Link
CVE-2023-34362	0.969370000	0.997350000	Link
CVE-2023-34039	0.945410000	0.992480000	Link
CVE-2023-3368	0.933870000	0.991050000	Link
CVE-2023-33246	0.972570000	0.998560000	Link
CVE-2023-32315	0.973600000	0.999060000	Link
CVE-2023-30625	0.938290000	0.991530000	Link
CVE-2023-30013	0.962250000	0.995350000	Link
CVE-2023-29300	0.969840000	0.997520000	Link
CVE-2023-29298	0.943950000	0.992230000	Link
CVE-2023-28771	0.918640000	0.989420000	Link
CVE-2023-28343	0.948520000	0.992980000	Link
CVE-2023-28121	0.923740000	0.989900000	Link
CVE-2023-27524	0.970400000	0.997680000	Link
CVE-2023-27372	0.973020000	0.998770000	Link
CVE-2023-27350	0.969800000	0.997500000	Link
CVE-2023-26469	0.932230000	0.990870000	Link
CVE-2023-26360	0.957000000	0.994400000	Link
CVE-2023-26035	0.967100000	0.996670000	Link
CVE-2023-25717	0.956860000	0.994370000	Link
CVE-2023-25194	0.970160000	0.997600000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963760000	0.995750000	Link
CVE-2023-24489	0.973550000	0.999030000	Link
CVE-2023-23752	0.948880000	0.993050000	Link
CVE-2023-23397	0.901800000	0.988220000	Link
CVE-2023-23333	0.963260000	0.995620000	Link
CVE-2023-22527	0.970550000	0.997730000	Link
CVE-2023-22518	0.965950000	0.996340000	Link
CVE-2023-22515	0.973330000	0.998930000	Link
CVE-2023-21839	0.956220000	0.994290000	Link
CVE-2023-21554	0.950840000	0.993320000	Link
CVE-2023-20887	0.971080000	0.997970000	Link
CVE-2023-1671	0.964510000	0.995910000	Link
CVE-2023-0669	0.971300000	0.998070000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 01 Jul 2024

[NEU] [hoch] IBM InfoSphere Information Server: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in IBM InfoSphere Information Server ausnutzen, um beliebigen Programmcode auszuführen, einen Cross-Site-Scripting-Angriff durchzuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu erzeugen und vertrauliche Informationen offenzulegen.

- Link

—

Mon, 01 Jul 2024

[NEU] [hoch] OpenSSH: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in OpenSSH ausnutzen, um beliebigen Programmcode mit root Rechten auszuführen.

- Link

—

Mon, 01 Jul 2024

[NEU] [hoch] Samsung Exynos: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Samsung Exynos ausnutzen, um Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Denial-of-Service- und möglicherweise DDoS-Angriffe durchzuführen und nicht näher spezifizierte Auswirkungen zu erzielen.

- Link

—

Mon, 01 Jul 2024

[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen gefährden die Integrität, Vertraulichkeit und Verfügbarkeit

Ein entfernter, authentisierter, entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Oracle MySQL ausnutzen, um dadurch die Integrität, Vertraulichkeit und Verfügbarkeit zu gefährden.

- Link

—

Mon, 01 Jul 2024

[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen gefährden die Integrität, Vertraulichkeit und Verfügbarkeit

Ein entfernter, authentisierter, entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Oracle MySQL ausnutzen, um dadurch die Integrität, Vertraulichkeit und Verfügbarkeit zu gefährden.

- Link

—

Mon, 01 Jul 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in cpio ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Mon, 01 Jul 2024

[UPDATE] [hoch] Red Hat Enterprise Linux/WebKitGTK: Mehrere Schwachstellen ermöglichen Ausführen von beliebigem Programmcode mit Benutzerrechten

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in WebKitGTK ausnutzen, um beliebigen Programmcode mit Benutzerrechten auszuführen.

- Link

—

Mon, 01 Jul 2024

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

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

- Link

—

Mon, 01 Jul 2024

[UPDATE] [hoch] Red Hat Enterprise Linux (flatpak): Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux in flatpak ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Mon, 01 Jul 2024

[UPDATE] [hoch] GStreamer: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in GStreamer ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder beliebigen Code auszuführen.

- Link

—

Mon, 01 Jul 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Mon, 01 Jul 2024

[UPDATE] [hoch] X.Org X11: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in X.Org X11 ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Mon, 01 Jul 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

—

Mon, 01 Jul 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

—

Mon, 01 Jul 2024

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

Ein Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um Dateien zu manipulieren, einen Denial-of-Service-Zustand zu verursachen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, seine Privilegien zu erweitern oder um weitere nicht spezifizierte Angriffe auszuführen.

- Link

—

Mon, 01 Jul 2024

[UPDATE] [hoch] Red Hat OpenShift Service Mesh Containers: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat OpenShift Service Mesh Containers ausnutzen, um Dateien zu manipulieren, einen ‘Denial of Service’-Zustand erzuegen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder weitere nicht spezifizierte Angriffe durchzuführen.

- Link

—

Mon, 01 Jul 2024

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

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

- Link

—

Mon, 01 Jul 2024

[UPDATE] [hoch] Avaya IP Office: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter Angreifer kann mehrere Schwachstellen in Avaya IP Office ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 01 Jul 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 offenzule-

gen oder Daten zu manipulieren.
- Link
—
Fri, 28 Jun 2024
[UPDATE] [hoch] Squid: Mehrere Schwachstellen
Ein entfernter, authentisierter oder anonymer Angreifer kann eine Schwachstelle in Squid ausnutzen, um Informationen offenzulegen und um einen Denial of Service Zustand herbeizuführen.
- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
7/1/2024	[GLSA-202407-03 : Liferea: Remote Code Execution]	critical
7/1/2024	[GLSA-202407-06 : cryptography: Multiple Vulnerabilities]	critical
7/1/2024	[GLSA-202407-08 : GNU Emacs, Org Mode: Multiple Vulnerabilities]	critical
7/1/2024	[Siemens Automation License Manager Path Traversal (CVE-2022-43514)]	critical
7/1/2024	[Splunk Enterprise 9.0.0 < 9.0.9, 9.1.0 < 9.1.4, 9.2.0 < 9.2.1 (SVD-2024-0718)]	critical
7/1/2024	[FreeBSD : netatalk3 – Multiple vulnerabilities (c742dbe8-3704-11ef-9e6e-b42e991fc52e)]	critical
7/1/2024	[Welotec Industrial Routers Improper Access Control (CVE-2023-1083)]	critical
7/1/2024	[RHEL 8 : pki-core (RHSA-2024:4179)]	high
7/1/2024	[Fedora 39 : mingw-gstreamer1 / mingw-gstreamer1-plugins-bad-free / etc (2024-919bc7e512)]	high
7/1/2024	[GLSA-202407-05 : SSSD: Command Injection]	high

Datum	Schwachstelle	Bewertung
7/1/2024	[GLSA-202407-02 : SDL_ttf: Arbitrary Memory Write]	high
7/1/2024	[GLSA-202407-04 : Pixman: Heap Buffer Overflow]	high
7/1/2024	[GLSA-202407-01 : Zsh: Prompt Expansion Vulnerability]	high
7/1/2024	[GLSA-202407-07 : cpio: Arbitrary Code Execution]	high
7/1/2024	[OpenSSH < 9.8 RCE]	high
7/1/2024	[Splunk Enterprise 9.0.0 < 9.0.10, 9.1.0 < 9.1.5, 9.2.0 < 9.2.2 (SVD-2024-0715)]	high
7/1/2024	[Apache 2.4.x < 2.4.60 Multiple Vulnerabilities]	high
7/1/2024	[Splunk Enterprise 9.0.0 < 9.0.10, 9.1.0 < 9.1.5, 9.2.0 < 9.2.2 (SVD-2024-0705)]	high
7/1/2024	[Splunk Enterprise 9.0.0 < 9.0.10, 9.1.0 < 9.1.5, 9.2.0 < 9.2.2 (SVD-2024-0704)]	high
7/1/2024	[Splunk Enterprise 9.0.0 < 9.0.10, 9.1.0 < 9.1.5, 9.2.0 < 9.2.2 (SVD-2024-0709)]	high
7/1/2024	[Splunk Enterprise 9.0.0 < 9.0.10, 9.1.0 < 9.1.5, 9.2.0 < 9.2.2 (SVD-2024-0703)]	high
7/1/2024	[Splunk Enterprise 9.0.0 < 9.0.10, 9.1.0 < 9.1.5, 9.2.0 < 9.2.2 (SVD-2024-0717)]	high
7/1/2024	[Ubuntu 22.04 LTS / 23.10 / 24.04 LTS : OpenSSH vulnerability (USN-6859-1)]	high
7/1/2024	[Oracle Linux 9 : openssh (ELSA-2024-12468)]	high
7/1/2024	[Debian dsa-5724 : openssh-client - security update]	high
7/1/2024	[FreeBSD : OpenSSH – Race condition resulting in potential remote code execution (f1a00122-3797-11ef-b611-84a93843eb75)]	high
7/1/2024	[Splunk Enterprise 9.0.0 < 9.0.10, 9.1.0 < 9.1.5, 9.2.0 < 9.2.2 (SVD-2024-0711)]	high
7/1/2024	[GLSA-202407-09 : OpenSSH: Remote Code Execution]	high
7/1/2024	[Slackware Linux 15.0 / current openssh Vulnerability (SSA:2024-183-01)]	high

Datum	Schwachstelle	Bewertung
7/1/2024	[Welotec Industrial Routers OS Command Injection (CVE-2023-1082)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Mon, 01 Jul 2024

Packet Storm New Exploits For June, 2024

This archive contains all of the 65 exploits added to Packet Storm in June, 2024.

- Link

—

” “Mon, 01 Jul 2024

OpenSSH Server regreSSHion Remote Code Execution

Qualys has discovered a a signal handler race condition vulnerability in OpenSSH’s server, sshd. If a client does not authenticate within LoginGraceTime seconds (120 by default, 600 in old OpenSSH versions), then sshd’s SIGALRM handler is called asynchronously, but this signal handler calls various functions that are not async-signal-safe - for example, syslog(). This race condition affects sshd in its default configuration.

- Link

—

” “Mon, 01 Jul 2024

Simple Laboratory Management System 1.0 SQL Injection

Simple Laboratory Management System version 1.0 suffers from a remote time-based SQL injection vulnerability.

- Link

—

” “Mon, 01 Jul 2024

Azon Dominator Affiliate Marketing Script SQL Injection

Azon Dominator Affiliate Marketing Script suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 01 Jul 2024

WordPress WPCode Lite 2.1.14 Cross Site Scripting

WordPress WPCode Lite plugin version 2.1.14 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Mon, 01 Jul 2024

Xhibiter NFT Marketplace 1.10.2 SQL Injection

Xhibiter NFT Marketplace version 1.10.2 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 01 Jul 2024

Customer Support System 1.0 Cross Site Scripting

Customer Support System version 1.0 suffers from a persistent cross site scripting vulnerability. Original discovery of cross site scripting in this version is attributed to Ahmed Abba in November of 2020.

- Link

—

” “Thu, 27 Jun 2024

SimpCMS 0.1 Cross Site Scripting

SimpCMS version 0.1 suffers from a cross site scripting vulnerability.

- Link

—

” “Wed, 26 Jun 2024

Ollama Remote Code Execution

Ollama versions prior to 0.1.34 suffer from a remote code execution vulnerability.

- Link

—

” “Wed, 26 Jun 2024

SolarWinds Platform 2024.1 SR1 Race Condition

SolarWinds Platform version 2024.1 SR1 suffers from a race condition vulnerability.

- Link

—

” “Wed, 26 Jun 2024

Automad 2.0.0-alpha.4 Cross Site Scripting

Automad version 2.0.0-alpha.4 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Wed, 26 Jun 2024

Poultry Farm Management System 1.0 Shell Upload

Poultry Farm Management System version 1.0 remote shell upload exploit. This is a variant of the original discovery of this flaw in this software version by Hejap Zairy in March of 2022.

- Link

—

” “Tue, 25 Jun 2024

Faronics WINSelect Hardcoded Credentials / Bad Permissions / Unhashed Password

Faronics WINSelect versions prior to 8.30.xx.903 suffer from having hardcoded credentials, storing unhashed passwords, and configuration file modification vulnerabilities.

- Link

—

” “Mon, 24 Jun 2024

Netis MW5360 Remote Command Execution

The Netis MW5360 router has a command injection vulnerability via the password parameter on the login page. The vulnerability stems from improper handling of the ”password” parameter within the router’s web interface. The router’s login page authorization can be bypassed by simply deleting the authorization header, leading to the vulnerability. All router firmware versions up to V1.0.1.3442 are vulnerable. Attackers can inject a command in the password parameter, encoded in base64, to exploit the command injection vulnerability. When exploited, this can lead to unauthorized command execution, potentially allowing the attacker to take control of the router.

- Link

—

” “Mon, 24 Jun 2024

Edu-Sharing Arbitrary File Upload

Edu-Sharing suffers from an arbitrary file upload vulnerability. Versions below 8.0.8-RC2, 8.1.4-RC0, and 9.0.0-RC19 are affected.

- Link

—

” “Mon, 24 Jun 2024

Flatboard 3.2 Cross Site Scripting

Flatboard version 3.2 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Mon, 24 Jun 2024

Carbon Forum 5.9.0 Cross Site Request Forgery / SQL Injection

Carbon Forum version 5.9.0 suffers from access control, cross site request forgery, file upload, outdated library, and remote SQL injection vulnerabilities.

- Link

—

” “Mon, 24 Jun 2024

Student Attendance Management System 1.0 SQL Injection

Student Attendance Management System version 1.0 suffers from a remote SQL Injection vulnerability that allows for authentication bypass.

- Link

—

” “Mon, 24 Jun 2024

Paradox IP150 Internet Module 1.40.00 Cross Site Request Forgery

Paradox IP150 Internet Module version 1.40.00 suffers from a cross site request forgery vulnerability.

- Link

—

” “Thu, 20 Jun 2024

TURPENTINE XNU Kernel Buffer Overflow

CVE-2024-27815 is a buffer overflow in the XNU kernel that was reported in sbconcat_mbufs. It was publicly fixed in xnu-10063.121.3, released with macOS 14.5, iOS 17.5, and visionOS 1.2. This bug was introduced in xnu-10002.1.13 (macOS 14.0/ iOS 17.0) and was fixed in xnu-10063.121.3 (macOS 14.5/ iOS 17.5). The bug affects kernels compiled with CONFIG_MBUF_MCACHE.

- Link

—

” “Wed, 19 Jun 2024

Bagisto 2.1.2 Client-Side Template Injection

Bagisto version 2.1.2 suffers from a client-side template injection vulnerability.

- Link

—

” “Wed, 19 Jun 2024

User Registration And Management System 3.2 SQL Injection

User Registration and Management System version 3.2 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Tue, 18 Jun 2024

PHP CGI Argument Injection Remote Code Execution

This Metasploit module exploits a PHP CGI argument injection vulnerability affecting PHP in certain configurations on a Windows target. A vulnerable configuration is locale dependant (such as Chinese or Japanese), such that the Unicode best-fit conversion scheme will unexpectedly convert a soft hyphen (0xAD) into a dash (0x2D) character. Additionally a target web server must be configured to run PHP under CGI mode, or directly expose the PHP binary. This issue has been fixed in PHP 8.3.8 (for the 8.3.x branch), 8.2.20 (for the 8.2.x branch), and 8.1.29 (for the 8.1.x branch). PHP 8.0.x and below

are end of life and have note received patches. XAMPP is vulnerable in a default configuration, and we can target the /php-cgi/php-cgi.exe endpoint. To target an explicit .php endpoint (e.g. /index.php), the server must be configured to run PHP scripts in CGI mode.

- Link

—

” “Tue, 18 Jun 2024

Apache OFBiz Forgot Password Directory Traversal

Apache OFBiz versions prior to 18.12.13 are vulnerable to a path traversal vulnerability. The vulnerable endpoint /webtools/control/forgotPassword allows an attacker to access the ProgramExport endpoint which in turn allows for remote code execution in the context of the user running the application.

- Link

—

” “Tue, 18 Jun 2024

PowerVR Out-Of-Bounds Write

PowerVR suffers from an out-of-bounds write of firmware addresses in PVRSRVRGXKickTA3DKM().

- Link

—

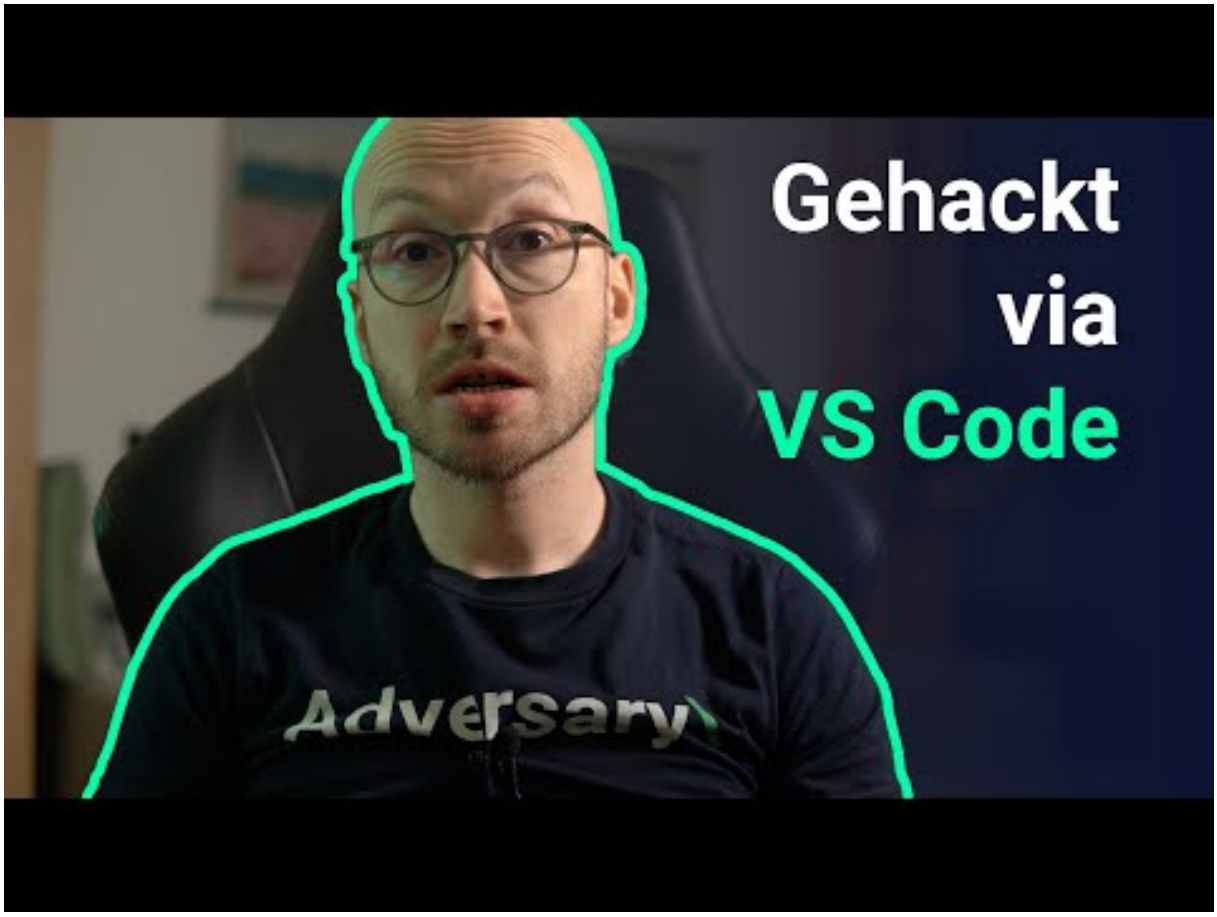
”

4.2 0-Days der letzten 5 Tage

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Die nächste Wahnsinns-Möglichkeit für Angreifer, Software-Unternehmen zu hacken (VSCode Extensions)



Zum Youtube Video

6 Cyberangriffe: (Jul)

Datum	Opfer	Land	Information

7 Ransomware-Erpressungen: (Jul)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-01	[Super Gardens]	dragonforce	Link
2024-07-01	[Hampden Veterinary Hospital]	dragonforce	Link
2024-07-01	[Indonesia Terkoneksi]	BrainCipher	Link
2024-07-01	[SYNERGY PEANUT]	akira	Link
2024-07-01	[Ethypharm]	underground	Link
2024-07-01	[latinusa.co.id]	lockbit3	Link
2024-07-01	[kbc-zagreb.hr]	lockbit3	Link
2024-07-01	[maxcess-logistics.com]	killsec	Link
2024-07-01	[Independent Education System]	handala	Link
2024-07-01	[Bartlett & Weigle Co. LPA.]	hunters	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.