
Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240605



Inhaltsverzeichnis

1 Editorial	2
2 Security-News	3
2.1 Heise - Security-Alert	3
3 Sicherheitslücken	4
3.1 EPSS	4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit	5
3.2 BSI - Warn- und Informationsdienst (WID)	7
3.3 Sicherheitslücken Meldungen von Tenable	11
4 Aktiv ausgenutzte Sicherheitslücken	13
4.1 Exploits der letzten 5 Tage	13
4.2 0-Days der letzten 5 Tage	17
5 Die Hacks der Woche	18
5.0.1 “Wir sind SeCuRiT Y hErStELLer”. Dann benehmt euch so ☒	18
6 Cyberangriffe: (Jun)	19
7 Ransomware-Erpressungen: (Jun)	19
8 Quellen	20
8.1 Quellenverzeichnis	20
9 Impressum	21

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

IT-Management-Plattform SolarWinds über mehrere Wege angreifbar

Die SolarWinds-Entwickler haben mehrere Sicherheitslücken in ihrer Software geschlossen. Angreifer können etwa für Abstürze sorgen.

- [Link](#)

—

Sicherheitsupdate: Schadcode-Attacken auf Autodesk AutoCAD möglich

Die CAD-Softwares Advance Steel, Civil 3D und AutoCAD von Autodesk sind verwundbar. Das Sicherheitsrisiko gilt als hoch.

- [Link](#)

—

Linux: root-Lücke wird aktiv missbraucht

Die IT-Sicherheitsbehörde CISA warnt vor aktiven Angriffen auf eine Linux-Lücke. Angreifer verschaffen sich damit root-Rechte.

- [Link](#)

—

IT-Monitoring: Checkmk schließt Lücke, die Änderung von Dateien ermöglicht

Eine Sicherheitslücke in der Monitoring-Software Checkmk ermöglicht Angreifern, unbefugt lokale Dateien auf dem Checkmk-Server zu lesen und zu schreiben.

- [Link](#)

—

Notfallpatch: Angreifer attackieren VPN-Verbindungen von Checkpoint Gateways

Checkpoint hat ein Notfall-Sicherheitsupdate veröffentlicht. Derzeit haben Angreifer Network Security Gateways wie Quantum Maestro im Visier.

- [Link](#)

—

Foxit PDF Reader: Halbherzige Zertifikatprüfung ermöglicht Rechteauserweiterung

Die Update-Routinen vom Foxit PDF Reader prüfen Zertifikate nicht richtig. Angreifer können dadurch ihre Rechte ausweiten.

- [Link](#)

—

Proof-of-Concept-Exploits für kritische FortiSIEM-Lücken: Jetzt patchen!

IT-Sicherheitsforscher haben für kritische Sicherheitslücken in FortiSIEM Proof-of-Concept-Exploits veröffentlicht. Höchste Zeit, die Updates zu installieren.

- [Link](#)

Supportende: Rechte-Sicherheitslücke gefährdet Ivanti Endpoint Manager 2021

Angrifer können Schadcode mit erhöhten Rechten ausführen. Admins müssen Ivanti EPM auf eine noch unterstützte Version upgraden.

- [Link](#)

Kritische Sicherheitslücke gewährt Angreifern Zugriff auf TP-Link-Router C5400X

Der TP-Link-WLAN-Router C5400X ist verwundbar. Ein Sicherheitspatch schließt eine kritische Schwachstelle.

- [Link](#)

Windows Server 2019: Aktualisiertes Sicherheitsupdate behebt Installationsfehler

Das Sicherheitsupdate für Windows Server 2019 schlug mit den Fehlernummern 0x800f0982 und 0x80004005 fehl. Ein aktualisiertes Update ist verfügbar.

- [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	0.959520000	0.994670000	Link
CVE-2023-6553	0.923550000	0.989600000	Link
CVE-2023-5360	0.965120000	0.995980000	Link
CVE-2023-4966	0.969890000	0.997400000	Link
CVE-2023-48795	0.959010000	0.994550000	Link
CVE-2023-47246	0.935450000	0.990940000	Link
CVE-2023-46805	0.963760000	0.995650000	Link
CVE-2023-46747	0.971460000	0.998040000	Link
CVE-2023-46604	0.931360000	0.990530000	Link
CVE-2023-4542	0.922430000	0.989470000	Link
CVE-2023-43208	0.963060000	0.995430000	Link
CVE-2023-43177	0.960230000	0.994820000	Link
CVE-2023-42793	0.970430000	0.997600000	Link
CVE-2023-41265	0.914120000	0.988830000	Link
CVE-2023-39143	0.948440000	0.992800000	Link
CVE-2023-38646	0.908390000	0.988380000	Link
CVE-2023-38205	0.938000000	0.991240000	Link
CVE-2023-38203	0.970370000	0.997580000	Link
CVE-2023-38146	0.905210000	0.988140000	Link
CVE-2023-38035	0.975020000	0.999830000	Link
CVE-2023-36845	0.966630000	0.996380000	Link
CVE-2023-3519	0.911860000	0.988680000	Link
CVE-2023-35082	0.968540000	0.997020000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-35078	0.968250000	0.996930000	Link
CVE-2023-34993	0.967190000	0.996540000	Link
CVE-2023-34960	0.933660000	0.990770000	Link
CVE-2023-34634	0.923550000	0.989610000	Link
CVE-2023-34362	0.961530000	0.995060000	Link
CVE-2023-34039	0.944630000	0.992180000	Link
CVE-2023-3368	0.928050000	0.990140000	Link
CVE-2023-33246	0.972320000	0.998400000	Link
CVE-2023-32315	0.973460000	0.998940000	Link
CVE-2023-32235	0.914550000	0.988860000	Link
CVE-2023-30625	0.950680000	0.993150000	Link
CVE-2023-30013	0.963050000	0.995430000	Link
CVE-2023-29300	0.969710000	0.997360000	Link
CVE-2023-29298	0.942510000	0.991770000	Link
CVE-2023-28771	0.918640000	0.989200000	Link
CVE-2023-28121	0.932700000	0.990680000	Link
CVE-2023-27524	0.971240000	0.997970000	Link
CVE-2023-27372	0.973630000	0.999020000	Link
CVE-2023-27350	0.971140000	0.997910000	Link
CVE-2023-26469	0.942400000	0.991760000	Link
CVE-2023-26360	0.952190000	0.993420000	Link
CVE-2023-26035	0.967700000	0.996770000	Link
CVE-2023-25717	0.956860000	0.994190000	Link
CVE-2023-25194	0.968000000	0.996860000	Link
CVE-2023-2479	0.963670000	0.995630000	Link
CVE-2023-24489	0.973760000	0.999070000	Link
CVE-2023-23752	0.932080000	0.990590000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23397	0.922480000	0.989480000	Link
CVE-2023-23333	0.963260000	0.995490000	Link
CVE-2023-22527	0.974590000	0.999580000	Link
CVE-2023-22518	0.962670000	0.995310000	Link
CVE-2023-22515	0.973130000	0.998750000	Link
CVE-2023-21839	0.959090000	0.994580000	Link
CVE-2023-21554	0.955760000	0.994010000	Link
CVE-2023-20887	0.965950000	0.996220000	Link
CVE-2023-20198	0.915340000	0.988940000	Link
CVE-2023-1698	0.912990000	0.988730000	Link
CVE-2023-1671	0.969090000	0.997150000	Link
CVE-2023-0669	0.969690000	0.997330000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 04 Jun 2024

[UPDATE] [hoch] Atlassian Confluence: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Atlassian Confluence ausnutzen, um beliebigen Programmcode auszuführen, um vertrauliche Informationen offenzulegen und um einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Tue, 04 Jun 2024

[NEU] [hoch] Fortra Tripwire: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Fortra Tripwire ausnutzen, um die Authentifizierung zu umgehen und dadurch Informationen offenlegen oder modifizieren.

- [Link](#)

—

Tue, 04 Jun 2024

[NEU] [hoch] Samsung Android: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Samsung Android ausnutzen, um seine Privilegien zu erweitern, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder Dateien zu manipulieren.

- [Link](#)

—

Tue, 04 Jun 2024

[NEU] [hoch] SolarWinds Platform: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in SolarWinds Platform ausnutzen, um Dateien zu manipulieren, einen Denial-of-Service-Zustand herbeizuführen oder einen Cross-Site-Scripting (XSS)-Angriff durchzuführen.

- [Link](#)

—

Tue, 04 Jun 2024

[NEU] [hoch] Android Patchday - June 2024: Mehrere Schwachstellen

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

- [Link](#)

—

Tue, 04 Jun 2024

[UPDATE] [kritisch] Oracle Fusion Middleware: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Oracle Fusion Middleware ausnutzen, um dadurch die Integrität, Vertraulichkeit und Verfügbarkeit zu gefährden.

- [Link](#)

—

Tue, 04 Jun 2024

[UPDATE] [hoch] python-cryptography: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonym Angreifer kann eine Schwachstelle in python-cryptography ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Tue, 04 Jun 2024

[UPDATE] [hoch] ffmpeg: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in ffmpeg ausnutzen, um einen Denial of Service Angriff durchzuführen, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.

- [Link](#)

—

Tue, 04 Jun 2024

[UPDATE] [hoch] OpenSSL: Mehrere Schwachstellen ermöglichen Denial of Service

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in OpenSSL ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.

- [Link](#)

—

Tue, 04 Jun 2024

[UPDATE] [hoch] Ruby: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Ruby ausnutzen, um Informationen offenzulegen oder Code auszuführen.

- [Link](#)

—

Tue, 04 Jun 2024

[UPDATE] [hoch] Microsoft Windows: Mehrere Schwachstellen

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Microsoft Windows 10, Microsoft Windows 11, Microsoft Windows Server, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019 und Microsoft Windows Server 2022 ausnutzen, um seine Privilegien zu erweitern, beliebigen Programmcode auszuführen, beliebigen Programmcode mit Administratorrechten auszuführen, Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen, einen Denial of Service Zustand herbeizuführen oder Dateien zu manipulieren

- [Link](#)

—

Tue, 04 Jun 2024

[UPDATE] [hoch] ffmpeg: Schwachstelle ermöglicht Codeausführung

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

- [Link](#)

—

Tue, 04 Jun 2024

[NEU] [hoch] Dell PowerScale: Schwachstelle ermöglicht Denial of Service und Offenlegung von Informationen

Ein Angreifer aus einem angrenzenden Netzwerk kann eine Schwachstelle in Dell PowerScale ausnutzen, um einen Denial of Service Zustand zu erzeugen und vertrauliche Informationen offenzulegen.

- [Link](#)

—

Mon, 03 Jun 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, 03 Jun 2024

[NEU] [hoch] Autodesk AutoCAD: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Autodesk AutoCAD ausnutzen, um beliebigen Programmcode auszuführen, um einen Denial-of-Service-Zustand zu erzeugen und um Dateien zu manipulieren.

- [Link](#)

—

Mon, 03 Jun 2024

[NEU] [hoch] Apache Wicket: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache Wicket ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Mon, 03 Jun 2024

[NEU] [hoch] Apache OFBiz: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache OFBiz ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Mon, 03 Jun 2024

[UPDATE] [hoch] Ruby: Schwachstelle ermöglicht Manipulation von Dateien

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Ruby ausnutzen, um Dateien zu manipulieren.

- [Link](#)

—

Mon, 03 Jun 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um beliebigen Programmcode auszuführen Informationen offenzulegen oder einen Denial of Service zu verursachen.

- [Link](#)

—

Mon, 03 Jun 2024

[UPDATE] [hoch] strongSwan: Schwachstelle ermöglicht Codeausführung und DoS

Ein entfernter, anonym Angreifer kann eine Schwachstelle in strongSwan ausnutzen, um beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
6/4/2024	[Progress Telerik Report Server Authentication Bypass (CVE-2024-4358)]	critical
6/4/2024	[Progress Telerik Report Server Insecure Deserialization (CVE-2024-1800)]	critical
6/3/2024	[RHEL 5 : less (Unpatched Vulnerability)]	critical
6/4/2024	[FreeBSD : chromium – multiple security fixes (b058380e-21a4-11ef-8a0f-a8a1599412c6)]	high
6/4/2024	[SUSE SLED12 / SLES12 Security Update : gstreamer-plugins-base (SUSE-SU-2024:1893-1)]	high
6/4/2024	[SUSE SLES15 Security Update : gstreamer-plugins-base (SUSE-SU-2024:1910-1)]	high
6/4/2024	[SUSE SLES12 Security Update : bind (SUSE-SU-2024:1894-1)]	high
6/4/2024	[openSUSE 15 Security Update : python-python-jose (openSUSE-SU-2024:0149-1)]	high
6/4/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : ffmpeg (SUSE-SU-2024:1908-1)]	high
6/4/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : glibc (SUSE-SU-2024:1895-1)]	high
6/4/2024	[Oracle Linux 9 : edk2 (ELSA-2024-23120)]	high
6/4/2024	[Oracle Linux 9 : edk2 (ELSA-2024-12409)]	high

Datum	Schwachstelle	Bewertung
6/4/2024	[Oracle Linux 9 : qemu-kvm (ELSA-2024-12407)]	high
6/4/2024	[RHEL 7 : glibc (RHSA-2024:3588)]	high
6/4/2024	[RHEL 8 : Red Hat JBoss Enterprise Application Platform 8.0.2 Security update (Moderate) (RHSA-2024:3580)]	high
6/4/2024	[RHEL 7 : 389-ds-base (RHSA-2024:3591)]	high
6/4/2024	[RHEL 9 : Red Hat JBoss Enterprise Application Platform 8.0.2 Security update (Moderate) (RHSA-2024:3581)]	high
6/4/2024	[Ubuntu 22.04 LTS / 23.10 / 24.04 LTS : libarchive vulnerability (USN-6805-1)]	high
6/4/2024	[Oracle Linux 7 : edk2 (ELSA-2024-12408)]	high
6/4/2024	[Oracle Linux 7 : 389-ds-base (ELSA-2024-3591)]	high
6/3/2024	[RHEL 8 : memcached (Unpatched Vulnerability)]	high
6/3/2024	[RHEL 4 : binutils (Unpatched Vulnerability)]	high
6/3/2024	[RHEL 9 : mod_security (Unpatched Vulnerability)]	high
6/3/2024	[RHEL 8 : mod_security (Unpatched Vulnerability)]	high
6/3/2024	[RHEL 7 : gdk-pixbuf (Unpatched Vulnerability)]	high
6/3/2024	[Microsoft Edge (Chromium) < 125.0.2535.85 Multiple Vulnerabilities]	high
6/3/2024	[RHEL 9 : nodejs (RHSA-2024:3545)]	high
6/3/2024	[RHEL 7 : Red Hat Single Sign-On 7.6.9 security update on RHEL 7 (Low) (RHSA-2024:3566)]	high
6/3/2024	[RHEL 9 : Red Hat Single Sign-On 7.6.9 security update on RHEL 9 (Low) (RHSA-2024:3568)]	high
6/3/2024	[RHEL 8 : Red Hat Single Sign-On 7.6.9 security update on RHEL 8 (Low) (RHSA-2024:3567)]	high
6/3/2024	[RHEL 9 : nodejs:18 (RHSA-2024:3544)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Tue, 04 Jun 2024

PowerVR DevmemXIntMapPages() Mapping Issue

PowerVR suffers from an issue where DevmemXIntMapPages() allows mapping sDevZeroPage/sDummyPage without holding reference.

- [Link](#)

—

” “Mon, 03 Jun 2024

Check Point Security Gateway Arbitrary File Read Detection Tool

This is a vulnerability detection and exploitation tool design to take in a list of targets and check for the arbitrary file read vulnerability in Check Point Security Gateways.

- [Link](#)

—

” “Mon, 03 Jun 2024

Check Point Security Gateway Arbitrary File Read

Proof of concept exploit for Check Point Security Gateways that allows an unauthenticated remote attacker to read the contents of an arbitrary file located on the affected appliance.

- [Link](#)

—

” “Mon, 03 Jun 2024

Employee And Visitor Gate Pass Logging System 1.0 SQL Injection

Employee and Visitor Gate Pass Logging System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Mon, 03 Jun 2024

FreePBX 16 Remote Code Execution

FreePBX suffers from a remote code execution vulnerability. Versions 14, 15, and 16 are all affected.

- [Link](#)

—

” “Mon, 03 Jun 2024

Sitefinity 15.0 Cross Site Scripting

Sitefinity version 15.0 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 03 Jun 2024

appRain CMF 4.0.5 Shell Upload

appRain CMF version 4.0.5 suffers from a remote shell upload vulnerability.

- [Link](#)

—

” “Mon, 03 Jun 2024

CMSimple 5.15 Remote Shell Upload

CMSimple version 5.15 suffers from a remote shell upload vulnerability.

- [Link](#)

—

” “Mon, 03 Jun 2024

Monstra CMS 3.0.4 Remote Code Execution

Monstra CMS version 3.0.4 suffers from a remote code execution vulnerability. Original discovery of code execution in this version is attributed to Ishaq Mohammed in December of 2017.

- [Link](#)

—

” “Mon, 03 Jun 2024

Dotclear 2.29 Remote Code Execution

Dotclear version 2.29 suffers from a remote code execution vulnerability.

- [Link](#)

—

” “Mon, 03 Jun 2024

WBCE CMS 1.6.2 Remote Code Execution

WBCE CME version 1.6.2 suffers from a remote code execution vulnerability.

- [Link](#)

—

” “Mon, 03 Jun 2024

Serendipity 2.5.0 Remote Code Execution

Serendipity version 2.5.0 suffers from a remote code execution vulnerability.

- [Link](#)

—

” “Fri, 31 May 2024

Packet Storm New Exploits For May, 2024

This archive contains all of the 68 exploits added to Packet Storm in May, 2024.

- [Link](#)

—

” “Fri, 31 May 2024

changedetection 0.45.20 Remote Code Execution

changedetection versions 0.45.20 and below suffer from a remote code execution vulnerability.

- [Link](#)

—

” “Fri, 31 May 2024

Online Payment Hub System 1.0 SQL Injection

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

- [Link](#)

—

” “Fri, 31 May 2024

BWL Advanced FAQ Manager 2.0.3 SQL Injection

BWL Advanced FAQ Manager version 2.0.3 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Fri, 31 May 2024

iMLog Cross Site Scripting

iMLog versions prior to 1.307 suffer from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Fri, 31 May 2024

Check Point Security Gateway Information Disclosure

Check Point Security Gateway suffers from an information disclosure vulnerability. Versions affected include R77.20 (EOL), R77.30 (EOL), R80.10 (EOL), R80.20 (EOL), R80.20.x, R80.20SP (EOL), R80.30 (EOL), R80.30SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x, and R81.20.

- [Link](#)

—

” “Thu, 30 May 2024

Aquatronica Control System 5.1.6 Password Disclosure

Aquatronica Control System version 5.1.6 has a tcp.php endpoint on the controller that is exposed to unauthenticated attackers over the network. This vulnerability allows remote attackers to send a POST request which can reveal sensitive configuration information, including plaintext passwords. This can lead to unauthorized access and control over the aquarium controller, compromising its security and potentially allowing attackers to manipulate its settings.

- [Link](#)

—

” “Thu, 30 May 2024

Progress Flowmon 12.3.5 Local sudo Privilege Escalation

This Metasploit module abuses a feature of the sudo command on Progress Flowmon. Certain binary

files are allowed to automatically elevate with the sudo command. This is based off of the file name. This includes executing a PHP command with a specific file name. If the file is overwritten with PHP code it can be used to elevate privileges to root. Progress Flowmon up to at least version 12.3.5 is vulnerable.

- [Link](#)

—

” “Thu, 30 May 2024

Akaunting 3.1.8 Client-Side Template Injection

Akaunting version 3.1.8 suffers from a client-side template injection vulnerability.

- [Link](#)

—

” “Thu, 30 May 2024

Akaunting 3.1.8 Server-Side Template Injection

Akaunting version 3.1.8 suffers from a server-side template injection vulnerability.

- [Link](#)

—

” “Thu, 30 May 2024

ORing IAP-420 2.01e Cross Site Scripting / Command Injection

ORing IAP-420 version 2.01e suffers from remote command injection and persistent cross site scripting vulnerabilities.

- [Link](#)

—

” “Wed, 29 May 2024

Flowmon Unauthenticated Command Injection

This Metasploit module exploits an unauthenticated command injection vulnerability in Progress Flowmon versions before v12.03.02.

- [Link](#)

—

” “Tue, 28 May 2024

Eclipse ThreadX Buffer Overflows

Eclipse ThreadX versions prior to 6.4.0 suffers from a missing array size check causing a memory overwrite, missing parameter checks leading to integer wraparound, under allocations, heap buffer overflows, and more.

- [Link](#)

—

”

4.2 0-Days der letzten 5 Tage

“Tue, 04 Jun 2024

ZDI-24-563: NETGEAR ProSAFE Network Management System UpLoadServlet Directory Traversal Remote Code Execution Vulnerability

- [Link](#)

—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 “Wir sind SeCuRiT y hErStELLer”. Dann benehmt euch so ☹



[Zum Youtube Video](#)

6 Cyberangriffe: (Jun)

Datum	Opfer	Land	Information
2024-06-04	Vietnam Post Corporation (Vietnam Post)	[VNM]	Link
2024-06-04	Synnovis	[GBR]	Link
2024-06-02	Institut technologique de Sonora (Itson)	[MEX]	Link

7 Ransomware-Erpressungen: (Jun)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-06-01	[Frontier.com]	ransomhub	Link
2024-06-04	[Premium Broking House]	SenSayQ	Link
2024-06-04	[Vimer Industrie Grafiche Italiane]	SenSayQ	Link
2024-06-04	[Voorhees Family Office Services]	everest	Link
2024-06-04	[Mahindra Racing]	akira	Link
2024-06-04	[naprodgroup.com]	lockbit3	Link
2024-06-03	[Madata Data Collection & Internet Portals]	mallox	Link
2024-06-03	[Río Negro]	mallox	Link
2024-06-03	[Langescheid GbR]	arcusmedia	Link
2024-06-03	[Franja IT Integradores de Tecnología]	arcusmedia	Link
2024-06-03	[Duque Saldarriaga]	arcusmedia	Link
2024-06-03	[BHMACH]	arcusmedia	Link
2024-06-03	[Botselo]	arcusmedia	Link
2024-06-03	[Immediate Transport – UK]	arcusmedia	Link
2024-06-01	[cfymca.org]	lockbit3	Link
2024-06-03	[Northern Minerals Limited]	bianlian	Link
2024-06-03	[ISETO CORPORATION]	8base	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-06-03	[Nidec Motor Corporation]	8base	Link
2024-06-03	[Anderson Mikos Architects]	akira	Link
2024-06-03	[My City application]	handala	Link
2024-06-02	[www.eastshoresound.com]	ransomhub	Link
2024-06-02	[smithandcaugheys.co.nz]	lockbit3	Link
2024-06-01	[Frontier]	ransomhub	Link
2024-06-16	[garrettmotion.com]	dispossessor	Link
2024-06-28	[notablefrontier.com]	dispossessor	Link
2024-06-12	[energytransfer.com]	dispossessor	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.