Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240607

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

Kritische DoS-Lücke bedroht IBM App Connect Enterprise Certified Container

Angreifer könnten IBM App Connect Enterprise Certified Container und DesignerAuthoring attackieren.

- Link

—

Sicherheitsupdates trotz Supportende: Zyxel sichert NAS-Systeme ab

Offensichtlich sind fünf jüngst entdeckte Lücken derart gefährlich, dass Zyxel sich um die EoL-Geräte kümmern muss.

- Link

—

Patchday: Attacken auf Geräte mit Android 12, 13 und 14 möglich

Wichtige Sicherheitsupdates schließen mehrere Schwachstellen in verschiedenen Android-Versionen.

- Link

—

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 Rechteausweitung
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

—

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	0.994690000	Link
CVE-2023-6553	0.918870000	0.989250000	Link
CVE-2023-5360	0.965120000	0.995990000	Link
CVE-2023-4966	0.969890000	0.997400000	Link
CVE-2023-48795	0.959010000	0.994580000	Link
CVE-2023-47246	0.935450000	0.990970000	Link
CVE-2023-46805	0.963760000	0.995660000	Link
CVE-2023-46747	0.971460000	0.998060000	Link
CVE-2023-46604	0.931360000	0.990580000	Link
CVE-2023-4542	0.922430000	0.989510000	Link
CVE-2023-43208	0.963060000	0.995450000	Link
CVE-2023-43177	0.960230000	0.994850000	Link
CVE-2023-42793	0.970430000	0.997600000	Link
CVE-2023-41265	0.914120000	0.988880000	Link
CVE-2023-39143	0.948440000	0.992830000	Link
CVE-2023-38646	0.908390000	0.988430000	Link
CVE-2023-38205	0.938000000	0.991270000	Link
CVE-2023-38203	0.970370000	0.997570000	Link
CVE-2023-38146	0.905210000	0.988190000	Link
CVE-2023-38035	0.975020000	0.999830000	Link
CVE-2023-36845	0.966630000	0.996400000	Link
CVE-2023-3519	0.911860000	0.988720000	Link
CVE-2023-35082	0.968540000	0.997030000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-35078	0.968250000	0.996940000	Link
CVE-2023-34993	0.967190000	0.996560000	Link
CVE-2023-34960	0.933660000	0.990810000	Link
CVE-2023-34634	0.923550000	0.989640000	Link
CVE-2023-34362	0.961530000	0.995100000	Link
CVE-2023-34039	0.944630000	0.992200000	Link
CVE-2023-3368	0.928050000	0.990180000	Link
CVE-2023-33246	0.972320000	0.998400000	Link
CVE-2023-32315	0.973460000	0.998940000	Link
CVE-2023-32235	0.902790000	0.988030000	Link
CVE-2023-30625	0.950680000	0.993180000	Link
CVE-2023-30013	0.963050000	0.995440000	Link
CVE-2023-29300	0.969710000	0.997350000	Link
CVE-2023-29298	0.942510000	0.991800000	Link
CVE-2023-28771	0.918640000	0.989240000	Link
CVE-2023-28121	0.932700000	0.990730000	Link
CVE-2023-27524	0.971240000	0.997970000	Link
CVE-2023-27372	0.973630000	0.999020000	Link
CVE-2023-27350	0.971140000	0.997900000	Link
CVE-2023-26469	0.942400000	0.991800000	Link
CVE-2023-26360	0.952190000	0.993440000	Link
CVE-2023-26035	0.967700000	0.996780000	Link
CVE-2023-25717	0.956860000	0.994220000	Link
CVE-2023-25194	0.968000000	0.996870000	Link
CVE-2023-2479	0.963670000	0.995640000	Link
CVE-2023-24489	0.973760000	0.999070000	Link
CVE-2023-23752	0.944080000	0.992060000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23397	0.922480000	0.989520000	Link
CVE-2023-23333	0.963260000	0.995500000	Link
CVE-2023-22527	0.974590000	0.999580000	Link
CVE-2023-22518	0.962670000	0.995340000	Link
CVE-2023-22515	0.973130000	0.998750000	Link
CVE-2023-21839	0.959090000	0.994610000	Link
CVE-2023-21554	0.955760000	0.994030000	Link
CVE-2023-20887	0.965950000	0.996230000	Link
CVE-2023-20198	0.915340000	0.989000000	Link
CVE-2023-1698	0.912990000	0.988770000	Link
CVE-2023-1671	0.969090000	0.997150000	Link
CVE-2023-0669	0.969690000	0.997330000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Thu, 06 Jun 2024

[NEU] [hoch] SysAid: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in SysAid Technologies Ltd SysAid ausnutzen, um eine SQL Injection durchzuführen oder beliebige Betriebssystemkommandos zu injizieren.

- Link

—

Thu, 06 Jun 2024

[UPDATE] [hoch] Ruby: Mehrere Schwachstellen

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

- Link

—

Thu, 06 Jun 2024

[UPDATE] [hoch] less: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Thu, 06 Jun 2024

[NEU] [hoch] Samsung Exynos: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer oder ein lokaler Angreifer mit hohen Privilegien kann mehrere Schwachstellen in Samsung Exynos ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen und Dateien zu manipulieren.

- Link

—

Thu, 06 Jun 2024

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

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

- Link

—

Thu, 06 Jun 2024

[UPDATE] [hoch] FRRouting Project FRRouting: Mehrere Schwachstellen ermöglichen Denial of Service

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in FRRouting Project FRRouting ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Thu, 06 Jun 2024

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

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

- Link

—

Thu, 06 Jun 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Squid ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Thu, 06 Jun 2024

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

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

- Link

—

Thu, 06 Jun 2024

[UPDATE] [hoch] Jenkins: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Jenkins ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder Cross-Site Scripting (XSS)-Angriffe durchzuführen.

- Link

—

Thu, 06 Jun 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Thu, 06 Jun 2024

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

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

- Link

—

Thu, 06 Jun 2024

[UPDATE] [hoch] Jenkins: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Jenkins ausnutzen, um Sicherheitsvorkehrungen zu umgehen, Informationen offenzulegen, Dateien zu manipulieren oder einen Cross-Site-Scripting-Angriff durchzuführen.

- Link

—

Thu, 06 Jun 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, seine Privilegien zu erweitern oder einen nicht spezifizierten Angriff durchzuführen.

- Link

—

Thu, 06 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

—

Thu, 06 Jun 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

—

Thu, 06 Jun 2024

[UPDATE] [kritisch] Tinyproxy: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Tinyproxy ausnutzen, um beliebigen Programmcode auszuführen und um vertrauliche Informationen offenzulegen.

- Link

—

Thu, 06 Jun 2024

[UPDATE] [hoch] Jenkins: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Jenkins ausnutzen, um beliebigen Code im Kontext des Dienstes auszuführen, Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.

- Link

—

Thu, 06 Jun 2024

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

Ein entfernter, anonymer 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

—

Wed, 05 Jun 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service zu verursachen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
6/6/2024	[PHP 8.3.x < 8.3.8 Multiple Vulnerabilities]	critical
6/6/2024	[PHP 8.2.x < 8.2.20 Multiple Vulnerabilities]	critical
6/6/2024	[PHP 8.1.x < 8.1.29 Multiple Vulnerabilities]	critical
6/6/2024	[Slackware Linux 15.0 / current php81 Multiple Vulnerabilities (SSA:2024-158-01)]	critical
6/5/2024	[F5 Networks BIG-IP : PyYAML vulnerability (K000139901)]	critical
6/7/2024	[RHEL 7 : booth (Unpatched Vulnerability)]	high
6/6/2024	[QEMU < 9.0.0 Multiple Vulnerabilities]	high
6/6/2024	[SolarWinds Platform < 2024.2 Multiple Vulnerabilities]	high
6/6/2024	[openSUSE 15 Security Update : python-PyMySQL (SUSE-SU-2024:1925-1)]	high
6/6/2024	[FreeBSD : cyrus-imapd – unbounded memory allocation (14908bda-232b-11ef-b621-00155d645102)]	high
6/6/2024	[RHEL 9 : booth (RHSA-2024:3660)]	high
6/6/2024	[RHEL 8 : booth (RHSA-2024:3658)]	high
6/6/2024	[RHEL 8 : tomcat (RHSA-2024:3666)]	high
6/6/2024	[RHEL 8 : booth (RHSA-2024:3657)]	high
6/6/2024	[RHEL 9 : booth (RHSA-2024:3661)]	high
6/6/2024	[RHEL 7 : less (RHSA-2024:3669)]	high
6/6/2024	[RHEL 8 : cockpit (RHSA-2024:3667)]	high
6/6/2024	[RHEL 8 : booth (RHSA-2024:3659)]	high
6/6/2024	[Fedora 39 : apptainer (2024-f4a65623e7)]	high

Datum	Schwachstelle	Bewertung
6/6/2024	[Oracle Linux 8 : kernel (ELSA-2024-3618)]	high
6/6/2024	[Oracle Linux 7 : less (ELSA-2024-3669)]	high
6/6/2024	[AlmaLinux 8 : tomcat (ALSA-2024:3666)]	high
6/6/2024	[AlmaLinux 8 : cockpit (ALSA-2024:3667)]	high
6/6/2024	[Oracle Linux 8 : cockpit (ELSA-2024-3667)]	high
6/6/2024	[Oracle Linux 8 : tomcat (ELSA-2024-3666)]	high
6/6/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : libvpx vulnerability (USN-6814-1)]	high
6/6/2024	[Ubuntu 24.04 LTS : AOM vulnerability (USN-6815-1)]	high
6/5/2024	[Slackware Linux 15.0 kernel-generic Multiple Vulnerabilities (SSA:2024-157-01)]	high
6/5/2024	[Oracle Linux 7 : glibc (ELSA-2024-3588)]	high
6/5/2024	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Atril vulnerability (USN-6808-1)]	high
6/5/2024	[Debian dsa-5706 : libarchive-dev - security update]	high
6/5/2024	[Fedora 40 : apptainer (2024-500c653b4c)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Thu, 06 Jun 2024

Boelter Blue System Management 1.3 SQL Injection

Boelter Blue System Management version 1.3 suffers from a remote SQL injection vulnerability.

- Link

—

” “Thu, 06 Jun 2024

Trojan.Win32.DarkGateLoader MVID-2024-0685 Code Execution

Multiple variants of Trojan.Win32.DarkGateLoader malware suffer from a code execution vulnerability.

- Link

—

” “Thu, 06 Jun 2024

Small CRM 1.0 SQL Injection

Small CRM version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Thu, 06 Jun 2024

Small CRM 1.0 Cross Site Scripting

Small CRM version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Thu, 06 Jun 2024

Northwind Demo 1.0 Cross Site Scripting

Northwind Demo version 1.0 suffers from persistent cross site scripting vulnerability.

- Link

—

” “Thu, 06 Jun 2024

WordPress Hash Form 1.1.0 Remote Code Execution

The Hash Form Drag and Drop Form Builder plugin for WordPress suffers from a critical vulnerability due to missing file type validation in the file_upload_action function. This vulnerability exists in all versions up to and including 1.1.0. Unauthenticated attackers can exploit this flaw to upload arbitrary files, including PHP scripts, to the server, potentially allowing for remote code execution on the affected WordPress site. This Metasploit module targets multiple platforms by adapting payload delivery and execution based on the server environment.

- Link

—

” “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

—

”

4.2 0-Days der letzten 5 Tage

“Thu, 06 Jun 2024

ZDI-24-582: SEW-EURODRIVE MOVITOOLS MotionStudio XML External Entity Processing Information Disclosure Vulnerability

- Link

—

” “Thu, 06 Jun 2024

ZDI-24-581: Microsoft Azure SQL Managed Instance Documentation SAS Token Incorrect Permission Assignment Authentication Bypass Vulnerability

- Link

—

” “Thu, 06 Jun 2024

ZDI-24-580: Microsoft Artifact Registry Container Images Empty Password Authentication Bypass Vulnerability

- Link

—

” “Thu, 06 Jun 2024

ZDI-24-579: Apple macOS PPM Image Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Thu, 06 Jun 2024

ZDI-24-578: Apple macOS CoreGraphics Image Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Thu, 06 Jun 2024

ZDI-24-577: Trend Micro Apex One Improper Access Control Local Privilege Escalation Vulnerability

- Link

—

” “Thu, 06 Jun 2024

ZDI-24-576: Trend Micro Maximum Security coreServiceShell Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Thu, 06 Jun 2024

ZDI-24-575: Trend Micro Deep Security Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Thu, 06 Jun 2024

ZDI-24-574: Trend Micro InterScan Web Security Virtual Appliance Cross-Site Scripting Privilege Escalation Vulnerability

- Link

—

” “Thu, 06 Jun 2024

ZDI-24-573: Trend Micro Apex One Security Agent Link Following Information Disclosure Vulnerability

- Link

—

” “Thu, 06 Jun 2024

ZDI-24-572: Trend Micro Apex One Security Agent Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Thu, 06 Jun 2024

ZDI-24-571: Trend Micro Apex One Security Agent Time-Of-Check Time-Of-Use Local Privilege Escalation Vulnerability

- Link

—

” “Thu, 06 Jun 2024

ZDI-24-570: Trend Micro Apex One Origin Validation Error Local Privilege Escalation Vulnerability

- Link

—

” “Thu, 06 Jun 2024

ZDI-24-569: Trend Micro Apex One Origin Validation Error Local Privilege Escalation Vulnerability

- Link

—

” “Thu, 06 Jun 2024

ZDI-24-568: Trend Micro Apex One Damage Cleanup Engine Link Following Denial-of-Service Vulnerability

- Link

—

” “Wed, 05 Jun 2024

ZDI-24-567: GStreamer AV1 Video Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Wed, 05 Jun 2024

ZDI-24-566: Luxion KeyShot Viewer KSP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Wed, 05 Jun 2024

ZDI-24-565: Luxion KeyShot Viewer KSP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Wed, 05 Jun 2024

ZDI-24-564: Fuji Electric Monitouch V-SFT V9 File Parsing Type Confusion Remote Code Execution Vulnerability

- Link

—

” “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 SeCuRitY hErsTeLlEr”. Dann benehmt euch so

Zum Youtube Video

6 Cyberangriffe: (Jun)

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

7 Ransomware-Erpressungen: (Jun)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-06	[RAVEN Mechanical]	hunters	Link
2024-06-06	[dmedelivers.com]	embargo	Link
2024-06-06	[fpr-us.com]	cactus	Link
2024-06-06	[TBMCG.com]	ElDorado	Link
2024-06-06	[www.vet.k-state.edu]	ElDorado	Link
2024-06-06	[www.uccretrievals.com]	ElDorado	Link
2024-06-06	[robson.com]	blackbasta	Link
2024-06-06	[elutia.com]	blackbasta	Link
2024-06-06	[ssiworld.com]	blackbasta	Link
2024-06-06	[driver-group.com]	blackbasta	Link
2024-06-06	[HTE Technologies]	ElDorado	Link
2024-06-06	[goughhomes.com]	ElDorado	Link
2024-06-06	[Baker Triangle]	ElDorado	Link
2024-06-06	[www.tankerska.hr]	ElDorado	Link
2024-06-06	[cityofpensacola.com]	ElDorado	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-06	[thunderbirdcc.org]	ElDorado	Link
2024-06-06	[www.itasnatta.edu.it]	ElDorado	Link
2024-06-06	[panzersolutions.com]	ElDorado	Link
2024-06-06	[lindostar.it]	ElDorado	Link
2024-06-06	[burotec.biz]	ElDorado	Link
2024-06-06	[celplan.com]	ElDorado	Link
2024-06-06	[adamshomes.com]	ElDorado	Link
2024-06-06	[dynasafe.com]	blackbasta	Link
2024-06-06	[Panasonic Australia]	akira	Link
2024-06-04	[Health People]	medusa	Link
2024-06-04	[IPPBX]	medusa	Link
2024-06-04	[Market Pioneer International Corp]	medusa	Link
2024-06-04	[Mercy Drive Inc]	medusa	Link
2024-06-04	[Radiosurgery New York]	medusa	Link
2024-06-04	[Inside Broadway]	medusa	Link
2024-06-04	[Oracle Advisory Services]	medusa	Link
2024-06-04	[Women’s Sports Foundation]	medusa	Link
2024-06-05	[“Moshe Kahn Advocates”]	mallox	Link
2024-06-05	[craigsteven.com]	lockbit3	Link
2024-06-05	[Elfi-Tech]	handala	Link
2024-06-05	[Dubai Municipality (UAE)]	daixin	Link
2024-06-05	[E-T-A]	akira	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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	[BHMAC]	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
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.