Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240608

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

Sicherheitspatch nachgebessert: Schadcode-Attacken auf PHP möglich

Angreifer können unter Windows den Schutz für eine PHP-Sicherheitslücke aus 2012 umgehen. Eigentlich sollte die Lücke längst geschlossen sein.

- Link

—

Kritische Azure-Lücke: Patch-Status derzeit unklar

Microsofts Cloud-Computing-Plattform Azure ist attackierbar. Sicherheitsforschern zufolge können Angreifer Schadcode auf Endpoints von Kunden ausführen.

- Link

—

Jetzt patchen! Exploitcode für kritische Lücke in Apache HugeGraph in Umlauf

Admins sollten aus Sicherheitsgründen das Tool zum Erstellen von Diagrammen HugeGraph von Apache zügig auf den aktuellen Stand bringen.

- Link

—

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

—

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	0.994710000	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	0.994590000	Link
CVE-2023-47246	0.935450000	0.990980000	Link
CVE-2023-46805	0.963760000	0.995660000	Link
CVE-2023-46747	0.971460000	0.998060000	Link
CVE-2023-46604	0.931360000	0.990590000	Link
CVE-2023-4542	0.922430000	0.989520000	Link
CVE-2023-43208	0.963060000	0.995450000	Link
CVE-2023-43177	0.960230000	0.994860000	Link
CVE-2023-42793	0.970430000	0.997600000	Link
CVE-2023-41265	0.914120000	0.988880000	Link
CVE-2023-39143	0.948440000	0.992840000	Link
CVE-2023-38646	0.908390000	0.988440000	Link
CVE-2023-38205	0.938000000	0.991280000	Link
CVE-2023-38203	0.970370000	0.997580000	Link
CVE-2023-38146	0.905210000	0.988200000	Link
CVE-2023-38035	0.975020000	0.999830000	Link
CVE-2023-36845	0.966630000	0.996410000	Link
CVE-2023-3519	0.909250000	0.988500000	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	0.996570000	Link
CVE-2023-34960	0.922740000	0.989560000	Link
CVE-2023-34634	0.923550000	0.989660000	Link
CVE-2023-34468	0.900570000	0.987890000	Link
CVE-2023-34362	0.961530000	0.995110000	Link
CVE-2023-34039	0.944630000	0.992210000	Link
CVE-2023-3368	0.928050000	0.990190000	Link
CVE-2023-33246	0.972320000	0.998400000	Link
CVE-2023-32315	0.973460000	0.998940000	Link
CVE-2023-32235	0.902790000	0.988050000	Link
CVE-2023-30625	0.950680000	0.993190000	Link
CVE-2023-30013	0.963050000	0.995450000	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	0.990750000	Link
CVE-2023-27524	0.971580000	0.998080000	Link
CVE-2023-27372	0.973630000	0.999020000	Link
CVE-2023-27350	0.971140000	0.997910000	Link
CVE-2023-26469	0.942400000	0.991800000	Link
CVE-2023-26360	0.952190000	0.993450000	Link
CVE-2023-26035	0.967700000	0.996780000	Link
CVE-2023-25717	0.956860000	0.994240000	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	EPSS	Perzentil	weitere Informationen
CVE-2023-23752	0.944080000	0.992070000	Link
CVE-2023-23397	0.922480000	0.989530000	Link
CVE-2023-23333	0.963260000	0.995510000	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	0.994620000	Link
CVE-2023-21554	0.955760000	0.994050000	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)

Fri, 07 Jun 2024

[NEU] [hoch] PHP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um beliebigen Programmcode auszuführen und um Sicherheitsmechanismen zu umgehen.

- Link

—

Fri, 07 Jun 2024

[UPDATE] [hoch] PostgreSQL JDBC Driver: Schwachstelle ermöglicht SQL-Injection

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PostgreSQL JDBC Driver ausnutzen, um eine SQL-Injection durchzuführen.

- Link

—

Fri, 07 Jun 2024

[UPDATE] [hoch] Ruby: Mehrere Schwachstellen

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

- Link

—

Fri, 07 Jun 2024

[UPDATE] [hoch] Roundcube: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Roundcube ausnutzen, um beliebige Kommandos auszuführen oder einen Cross-Site Scripting (XSS) Angriff durchzuführen.

- Link

—

Fri, 07 Jun 2024

[NEU] [hoch] Roundcube: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Roundcube ausnutzen, um einen Cross-Site Scripting Angriff zu starten oder beliebigen Code auszuführen.

- Link

—

Fri, 07 Jun 2024

[UPDATE] [hoch] OpenJDK: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in OpenJDK ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsvorkehrungen zu umgehen oder Dateien zu manipulieren.

- Link

—

Fri, 07 Jun 2024

[UPDATE] [hoch] QEMU: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in QEMU ausnutzen, um seine Privilegien zu erhöhen, Code auszuführen oder einen Denial of Service zu verursachen.

- Link

—

Fri, 07 Jun 2024

[UPDATE] [hoch] Red Hat JBoss A-MQ: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat JBoss A-MQ und Red Hat Enterprise Linux ausnutzen, um Informationen offenzulegen oder beliebigen Programmcode auszuführen.

- Link

—

Fri, 07 Jun 2024

[UPDATE] [hoch] VMware Tanzu Spring Framework: Schwachstelle ermöglicht Manipulation von Daten

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in VMware Tanzu Spring Framework ausnutzen, um Daten zu manipulieren oder Informationen offenzulegen.

- Link

—

Fri, 07 Jun 2024

[UPDATE] [hoch] less: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Fri, 07 Jun 2024

[NEU] [UNGEPATCHT] [kritisch] Microsoft Azure: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Microsoft Azure ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 07 Jun 2024

[NEU] [UNGEPATCHT] [hoch] HCL Domino: Schwachstelle ermöglicht Cross-Site Scripting

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in HCL Domino ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen.

- Link

—

Fri, 07 Jun 2024

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

Ein Angreifer kann mehrere Schwachstellen in IBM QRadar SIEM ausnutzen, um Dateien zu manipulieren, um einen Denial-of-Service-Zustand erzuegen, um vertrauliche Informationen offenzulegen, um die Sicherheitsmaßnahmen zu umgehen und beliebigen Code auszuführen.

- Link

—

Fri, 07 Jun 2024

[NEU] [hoch] SolarWinds Serv-U Managed File Transfer Server: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in SolarWinds Serv-U Managed File Transfer Server ausnutzen, um Informationen offenzulegen.

- Link

—

Fri, 07 Jun 2024

[NEU] [hoch] Samsung Exynos: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Samsung Exynos ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 07 Jun 2024

[NEU] [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

—

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

[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
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
6/7/2024	[OpenSSL 0.9.8 < 0.9.8p Vulnerability]	critical
6/7/2024	[OpenSSL 0.9.8h < 0.9.8o Vulnerability]	critical
6/7/2024	[OpenSSL 0.9.8v < 0.9.8w Vulnerability]	critical
6/7/2024	[OpenSSL 0.9.8h < 0.9.8r Vulnerability]	critical
6/7/2024	[OpenSSL 1.0.0 < 1.0.0b Vulnerability]	critical
6/7/2024	[RHEL 7 : booth (Unpatched Vulnerability)]	high
6/7/2024	[SolarWinds Serv-U 15.4.2 < 15.4.3]	high
6/7/2024	[Autodesk Multiple Vulnerabilities (AutoCAD) (adsk-sa-2024-0009)]	high
6/7/2024	[Juniper Junos OS Vulnerability (JSA79095)]	high
6/7/2024	[Ollama < 0.1.29 DNS Rebinding]	high
6/7/2024	[OpenSSL 0.9.7 < 0.9.7k Vulnerability]	high
6/7/2024	[OpenSSL 0.9.7 < 0.9.7d Multiple Vulnerabilities]	high
6/7/2024	[OpenSSL 0.9.8 < 0.9.8d Multiple Vulnerabilities]	high
6/7/2024	[OpenSSL 0.9.6c < 0.9.6m Vulnerability]	high
6/7/2024	[OpenSSL 0.9.6 < 0.9.6d Vulnerability]	high
6/7/2024	[OpenSSL 0.9.8 < 0.9.8q Vulnerability]	high
6/7/2024	[OpenSSL 0.9.7 < 0.9.7l Multiple Vulnerabilities]	high
6/7/2024	[OpenSSL 0.9.8 < 0.9.8c Vulnerability]	high
6/7/2024	[Juniper Junos OS Vulnerability (JSA79092)]	high

Datum	Schwachstelle	Bewertung
6/7/2024	[libndp >= 1.0 Buffer Overflow]	high
6/7/2024	[Cisco Firepower Management Center Software SQL Injection (cisco-sa-fmc-sqli-WFFDnNOs)]	high
6/7/2024	[Ubuntu 22.04 LTS / 23.10 : Linux kernel vulnerabilities (USN-6818-1)]	high
6/7/2024	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6820-1)]	high
6/7/2024	[Ubuntu 22.04 LTS / 23.10 : Linux kernel vulnerabilities (USN-6819-1)]	high
6/7/2024	[Ubuntu 22.04 LTS : Linux kernel vulnerabilities (USN-6821-1)]	high
6/7/2024	[Ubuntu 24.04 LTS : Linux kernel vulnerabilities (USN-6817-1)]	high
6/7/2024	[Ubuntu 24.04 LTS : Linux kernel vulnerabilities (USN-6816-1)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Fri, 07 Jun 2024

Online Pizza Ordering System 1.0 SQL Injection

Online Pizza Ordering System version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Fri, 07 Jun 2024

Apache HugeGraph Remote Command Execution

Apache HugeGraph versions 1.0.0 and up to 1.3.0 suffer from a remote command execution vulnerability. This is a scanner to test for the issue.

- Link

—

” “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
—
”

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
2024-06-08	[Hoppecke]	dragonforce	Link
2024-06-07	[Elite Limousine Plus Inc]	bianlian	Link
2024-06-07	[ccmaui.org]	lockbit3	Link
2024-06-07	[talalayglobal.com]	blackbasta	Link
2024-06-07	[akdenizchemson.com]	blackbasta	Link
2024-06-07	[Reinhold Sign Service]	akira	Link
2024-06-07	[Axip Energy Services]	hunters	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.