Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240817

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

Zoom schützt Anwendungen unter Linux, macOS und Windows vor möglichen Attacken
Es sind wichtige Sicherheitsupdates für unter anderem Zoom Workplace und Rooms Client erschienen.
- Link

—

Sicherheitsupdates F5: Angreifer können unbefugt auf BIG-IP-Appliances zugreifen
Mehrere Sicherheitslücken ermöglichen Attacken auf BIG-IP Next Central Manager und BIG-IP Next SPK.
- Link

—

Solarwinds Web Help Desk: Schadcode kann Host-System infizieren
Eine nun geschlossene kritische Sicherheitslücke bedrohte die Kundensupport-Software Web Help Desk von Solarwinds.
- Link

—

IBM-Entwickler schließen Schadcode-Lücken in AIX und App Connect
Unternehmen mit IBM-Software sollten ihre Systeme aus Sicherheitsgründen auf den aktuellen Stand bringen.
- Link

—

Ivanti schließt unter anderem Admin-Lücke in Virtual Traffic Manager
Kritische Sicherheitslücken bedrohen Produkte von Ivanti. Noch sind keine Attacken bekannt. Noch sind nicht alle Updates verfügbar.
- Link

—

Patchday Adobe: Acrobat, Illustrator & Co. als Schlupfloch für Schadcode
Adobe stuft mehrere Sicherheitslücken in seinen Produkten als kritisch ein. Sicherheitsupdates sind verfügbar.
- Link

—

Patchday Microsoft: Angreifer attackieren Office und Windows mit Schadcode
Es sind wichtige Sicherheitsupdates für verschiedene Microsoft-Produkte erschienen. Aufgrund von laufenden Attacken sollten Admins zügig handeln.
- Link

—

Patchday: Angreifer können SAP BusinessObjects kompromittieren

Die SAP-Entwickler haben unter anderem kritische Sicherheitslücken in ihrer Unternehmenssoftware geschlossen.

- Link

—

Sicherheitslücken: Netzwerkmonitoringtool Zabbix kann Passwörter leaken

Unter anderen eine kritische Schadcode-Lücke bedroht Zabbix. Dagegen abgesicherte Versionen stehen zum Download bereit.

- Link

—

Root-Sicherheitslücke bedroht Datenbankmanagementsystem PostgreSQL

Die PostgreSQL-Entwickler haben in aktuellen Versionen eine Schwachstelle geschlossen. Angreifer können Schadcode ausführen.

- 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-2023-6895	0.921160000	0.989980000	Link
CVE-2023-6553	0.927320000	0.990700000	Link
CVE-2023-5360	0.902780000	0.988740000	Link
CVE-2023-52251	0.944080000	0.992550000	Link
CVE-2023-4966	0.971280000	0.998290000	Link
CVE-2023-49103	0.962110000	0.995600000	Link
CVE-2023-48795	0.965330000	0.996430000	Link
CVE-2023-47246	0.959010000	0.995010000	Link
CVE-2023-46805	0.937250000	0.991710000	Link
CVE-2023-46747	0.972820000	0.998880000	Link
CVE-2023-46604	0.961790000	0.995530000	Link
CVE-2023-4542	0.928310000	0.990800000	Link
CVE-2023-43208	0.972240000	0.998630000	Link
CVE-2023-43177	0.964550000	0.996180000	Link
CVE-2023-42793	0.969020000	0.997460000	Link
CVE-2023-41265	0.911110000	0.989280000	Link
CVE-2023-39143	0.939130000	0.991960000	Link
CVE-2023-38646	0.906610000	0.988980000	Link
CVE-2023-38205	0.953670000	0.994110000	Link
CVE-2023-38203	0.966410000	0.996720000	Link
CVE-2023-38146	0.920720000	0.989940000	Link
CVE-2023-38035	0.974920000	0.999810000	Link
CVE-2023-36845	0.966270000	0.996680000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3519	0.965340000	0.996440000	Link
CVE-2023-35082	0.966130000	0.996630000	Link
CVE-2023-35078	0.970440000	0.997950000	Link
CVE-2023-34993	0.973130000	0.999010000	Link
CVE-2023-34960	0.928290000	0.990790000	Link
CVE-2023-34634	0.925130000	0.990470000	Link
CVE-2023-34468	0.906650000	0.988990000	Link
CVE-2023-34362	0.971000000	0.998180000	Link
CVE-2023-34039	0.947770000	0.993090000	Link
CVE-2023-3368	0.932420000	0.991260000	Link
CVE-2023-33246	0.972040000	0.998520000	Link
CVE-2023-32315	0.970550000	0.998000000	Link
CVE-2023-30625	0.953800000	0.994130000	Link
CVE-2023-30013	0.962380000	0.995660000	Link
CVE-2023-29300	0.968930000	0.997440000	Link
CVE-2023-29298	0.947600000	0.993060000	Link
CVE-2023-28432	0.906190000	0.988930000	Link
CVE-2023-28343	0.942300000	0.992330000	Link
CVE-2023-28121	0.909500000	0.989140000	Link
CVE-2023-27524	0.970600000	0.998020000	Link
CVE-2023-27372	0.972120000	0.998570000	Link
CVE-2023-27350	0.969720000	0.997730000	Link
CVE-2023-26469	0.956020000	0.994560000	Link
CVE-2023-26360	0.965230000	0.996390000	Link
CVE-2023-26035	0.967360000	0.996990000	Link
CVE-2023-25717	0.954250000	0.994220000	Link
CVE-2023-25194	0.968820000	0.997420000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963740000	0.995970000	Link
CVE-2023-24489	0.973870000	0.999300000	Link
CVE-2023-23752	0.956380000	0.994600000	Link
CVE-2023-23333	0.962300000	0.995640000	Link
CVE-2023-22527	0.968290000	0.997250000	Link
CVE-2023-22518	0.965970000	0.996580000	Link
CVE-2023-22515	0.973250000	0.999060000	Link
CVE-2023-21839	0.955020000	0.994360000	Link
CVE-2023-21554	0.952830000	0.993960000	Link
CVE-2023-20887	0.970670000	0.998040000	Link
CVE-2023-1671	0.962480000	0.995660000	Link
CVE-2023-0669	0.969760000	0.997740000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 16 Aug 2024

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

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in IBM QRadar SIEM ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen und einen Cross-Site-Scripting-Angriff durchzuführen.

- Link

—

Fri, 16 Aug 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.

- Link

—

Fri, 16 Aug 2024

[UPDATE] [hoch] Foxit PDF Editor: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Foxit PDF Editor ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu erzeugen und vertrauliche Informationen preiszugeben.

- Link

—

Fri, 16 Aug 2024

[UPDATE] [hoch] Mozilla Firefox, Firefox ESR und Thunderbird: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um einen Spoofing-Angriff durchzuführen, beliebigen Code auszuführen, Dateien zu manipulieren, vertrauliche Informationen offenzulegen oder Cross-Site-Scripting-Angriffe durchzuführen.

- Link

—

Fri, 16 Aug 2024

[UPDATE] [hoch] Zabbix: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Zabbix ausnutzen, um Informationen offenzulegen, Dateien zu manipulieren, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen oder beliebigen Code auszuführen.

- Link

—

Fri, 16 Aug 2024

[UPDATE] [hoch] Intel Ethernet Controller: Mehrere Schwachstellen ermöglichen Privilegieneskalation und Denial of Service

Ein lokaler oder entfernter anonymer Angreifer kann mehrere Schwachstellen in Intel Ethernet Controller ausnutzen, um seine Privilegien zu erhöhen und einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Thu, 15 Aug 2024

[NEU] [hoch] Red Hat Enterprise Linux (Fence Agents Remediation): Schwachstelle ermöglicht Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 15 Aug 2024

[UPDATE] [UNGEPATCHT] [hoch] Ivanti Connect Secure und Fortinet FortiGate: Mehrere Schwachstellen ermöglichen Manipulation von Dateien und die Offenlegung von Informationen

Ein Angreifer mit Zugriff auf das System kann mehrere Schwachstellen in Ivanti Connect Secure und Fortinet FortiGate ausnutzen, um Dateien zu manipulieren und vertrauliche Informationen preiszugeben.

- Link

—

Thu, 15 Aug 2024

[NEU] [hoch] PaloAlto Networks Cortex XSOAR: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PaloAlto Networks Cortex XSOAR ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 15 Aug 2024

[UPDATE] [hoch] Intel Server Board S2600ST Family Firmware: Schwachstelle ermöglicht Privilegieneskalation

Ein lokaler Angreifer kann eine Schwachstelle in der Intel Server Board S2600ST Family Firmware ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Thu, 15 Aug 2024

[UPDATE] [hoch] Jenkins Plugins: Mehrere Schwachstellen

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

- Link

—

Thu, 15 Aug 2024

[UPDATE] [hoch] BusyBox: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Thu, 15 Aug 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, 15 Aug 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder um Sicherheitsmaßnahmen zu umgehen.

- Link

—

Thu, 15 Aug 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder einen 'Denial of Service'-Zustand zu verursachen.

- Link

—

Thu, 15 Aug 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um Sicherheitsvorkehrungen zu umgehen und um Dateien zu manipulieren.

- Link

—

Thu, 15 Aug 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 offenzulegen oder Daten zu manipulieren.

- Link

—

Thu, 15 Aug 2024

[UPDATE] [hoch] OpenSSH: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Thu, 15 Aug 2024

[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.

- Link

—

Thu, 15 Aug 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

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/16/2024	[SUSE SLES15 Security Update : openssl-3 (SUSE-SU-2024:2931-1)]	critical
8/16/2024	[CBL Mariner 2.0 Security Update: packer (CVE-2023-49569)]	critical
8/16/2024	[SUSE SLED15 / SLES15 Security Update : zziplib (SUSE-SU-2024:2925-1)]	high
8/16/2024	[SUSE SLES15 Security Update : kernel (SUSE-SU-2024:2923-1)]	high
8/16/2024	[SUSE SLES15 Security Update : kernel (SUSE-SU-2024:2929-1)]	high
8/16/2024	[openSUSE 15 Security Update : opera (openSUSE-SU-2024:0242-1)]	high
8/16/2024	[SUSE SLED12 / SLES12 Security Update : zziplib (SUSE-SU-2024:2926-1)]	high
8/16/2024	[Fedora 40 : tor (2024-3f9eb3c86c)]	high
8/16/2024	[Schneider Electric Accutech Manager Buffer Overflow]	high
8/16/2024	[Schneider Electric Accutech Manager Buffer Overflow]	high
8/16/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2010-4563)]	high
8/16/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-36971)]	high

Datum	Schwachstelle	Bewertung
8/16/2024	[CBL Mariner 2.0 Security Update: httpd (CVE-2024-24795)]	high
8/16/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2007-4998)]	high
8/16/2024	[CBL Mariner 2.0 Security Update: httpd (CVE-2024-27316)]	high
8/16/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2010-0309)]	high
8/16/2024	[CBL Mariner 2.0 Security Update: hyperv-daemons / kernel (CVE-2024-0565)]	high
8/16/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2023-6931)]	high
8/16/2024	[CBL Mariner 2.0 Security Update: packer (CVE-2023-49568)]	high
8/16/2024	[CBL Mariner 2.0 Security Update: libtiff (CVE-2023-52356)]	high
8/16/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2010-0298)]	high
8/16/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-21803)]	high
8/16/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-0646)]	high
8/16/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-26952)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Thu, 15 Aug 2024

LG Simple Editor 3.21.0 Command Injection

LG Simple Editor versions 3.21.0 and below suffer from an unauthenticated command injection vulnerability. The vulnerability can be exploited by a remote attacker to inject arbitrary operating system commands which will get executed in the context of NT AUTHORITY\SYSTEM.

- Link

—

” “Thu, 15 Aug 2024

OpenMetadata 1.2.3 Authentication Bypass / SpEL Injection

This Metasploit module exploits OpenMetadata versions 1.2.3 and below by chaining an API authentication bypass using JWT tokens along with a SpEL injection vulnerability to achieve arbitrary command execution.

- Link

—

” “Thu, 15 Aug 2024

Apache HugeGraph Gremlin Remote Code Execution

This Metasploit module exploits CVE-2024-27348, a remote code execution vulnerability that exists in Apache HugeGraph Server in versions before 1.3.0. An attacker can bypass the sandbox restrictions and achieve remote code execution through Gremlin, resulting in complete control over the server.

- Link

—

” “Thu, 15 Aug 2024

Feberr 13.4 Insecure Settings

Feberr version 13.4 suffers from an ignored default credential vulnerability.

- Link

—

” “Thu, 15 Aug 2024

Farmacia Gama 1.0 Cross Site Scripting

Farmacia Gama version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Thu, 15 Aug 2024

Ecommerce 1.15 Insecure Settings

Ecommerce version 1.15 suffers from an ignored default credential vulnerability.

- Link

—

” “Thu, 15 Aug 2024

Covid-19 Contact Tracing System 1.0 Cross Site Scripting

Covid-19 Contact Tracing System version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Thu, 15 Aug 2024

Car Rental Management System 1.0 Cross Site Scripting

Car Rental Management System version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Thu, 15 Aug 2024

BloodBank 1.1 Insecure Settings

BloodBank version 1.1 suffers from an ignored default credential vulnerability.

- Link

—

” “Thu, 15 Aug 2024

Bhojon Restaurant Management System 2.9 Insecure Settings

Bhojon Restaurant Management System version 2.9 suffers from an ignored default credential vulnerability.

- Link

—

” “Thu, 15 Aug 2024

FlatPress 1.3.1 Path Traversal

FlatPress version 1.3.1 suffers from a path traversal vulnerability.

- Link

—

” “Wed, 14 Aug 2024

K7 Ultimate Security NULL Pointer Dereference

In K7 Ultimate Security versions prior to 17.0.2019, the driver file (K7RKScan.sys - this version 15.1.0.7) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of a null pointer dereference from IOCtl 0x222010 and 0x222014. At the same time, the drive is accessible to all users in the ”Everyone” group.

- Link

—

” “Wed, 14 Aug 2024

Microsoft CLFS.sys Denial of Service

CVE-2024-6768 is a vulnerability in the Common Log File System (CLFS.sys) driver of Windows, caused by improper validation of specified quantities in input data. This flaw leads to an unrecoverable inconsistency, triggering the KeBugCheckEx function and resulting in a Blue Screen of Death (BSoD). The issue affects all versions of Windows 10 and Windows 11, Windows Server 2016, Server 2019 and Server 2022 despite having all updates applied. This Proof of Concept (PoC) shows that by crafting specific values within a .BLF file, an unprivileged user can induce a system crash.

- Link

—

” “Wed, 14 Aug 2024

Kortex 1.0 Insecure Direct Object Reference

Kortex version 1.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Wed, 14 Aug 2024

Job Castle 1.0 Arbitrary File Upload

Job Castle version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Wed, 14 Aug 2024

Hotel Management System 1.0 Arbitrary File Upload

Hotel Management System version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Wed, 14 Aug 2024

Covid-19 Contact Tracing System 1.0 SQL Injection

Covid-19 Contact Tracing System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Wed, 14 Aug 2024

Car Listing 1.6 Insecure Settings

Car Listing version 1.6 suffers from an ignored default credential vulnerability.

- Link

—

” “Wed, 14 Aug 2024

MalwareBytes 19 Arbitrary File Deletion / Privilege Escalation

Malwarebytes is prone to an arbitrary file deletion (usage of DeleteFileW by MBAMService.exe) running as SYSTEM. This process can be manipulated from a non-admin user because it fails to properly filter the user supplied input while scanning a file, this vulnerability leads to a privilege escalation. This exploit was tested on Windows 10 Pro version 22H2 (OS Build 19045.4412). Versions 19 and below are affected.

- Link

—

” “Tue, 13 Aug 2024

WordPress MapFig Studio 0.2.1 Cross Site Request Forgery / Cross Site Scripting

WordPress MapFig Studio plugin versions 0.2.1 and below suffer from cross site request forgery and cross site scripting vulnerabilities.

- Link

—

” “Tue, 13 Aug 2024

WordPress Profilepro 1.3 Cross Site Scripting

WordPress Profilepro plugin versions 1.3 and below suffer from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 13 Aug 2024

WordPress Light Poll 1.0.0 Cross Site Request Forgery

WordPress Light Poll plugin versions 1.0.0 and below suffer from multiple cross site request forgery vulnerabilities.

- Link

—

” “Tue, 13 Aug 2024

WordPress PVN Auth Popup 1.0.0 Cross Site Scripting

WordPress PVN Auth Popup plugin version 1.0.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 13 Aug 2024

Giftora 1.0 Cross Site Request Forgery

Giftora version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Tue, 13 Aug 2024

Gas Agency Management 2022 Shell Upload

Gas Agency Management version 2022 suffers from a remote shell upload vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Thu, 15 Aug 2024

ZDI-24-1151: Ivanti Avalanche WLAvalancheService Null Pointer Dereference Denial-of-Service Vulnerability

- Link

—

” “Thu, 15 Aug 2024

ZDI-24-1150: Ivanti Avalanche decodeToMap XML External Entity Processing Information Disclosure Vulnerability

- Link

—

” “Thu, 15 Aug 2024

ZDI-24-1149: Ivanti Avalanche deleteSkin Directory Traversal Arbitrary File Deletion Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1148: Microsoft Office PowerPoint PPTX File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1147: Microsoft Windows 10 WinREUpdateInstaller_2401B_amd64 Link Following Privilege Escalation Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1146: Microsoft Windows 10 WinREUpdateInstaller DLL Hijacking Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1145: Microsoft Office Visio VSDX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1144: Adobe Substance 3D Stager SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1143: Adobe Dimension SKP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1142: Adobe Dimension SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1141: Adobe Dimension GLB File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1140: Adobe Dimension USD File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1139: Adobe Bridge AVI FIle Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1138: Adobe Bridge JP2 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1137: Adobe Bridge AVI FIle Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1136: Adobe Acrobat Reader DC AcroForm Annotation Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1135: Adobe Acrobat Reader DC AcroForm Annotation Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1134: Adobe Acrobat Reader DC Annotation Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1133: Adobe Acrobat Reader DC AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1132: Adobe Acrobat Reader DC Annotation Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1131: Adobe Acrobat Reader DC Annotation Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1130: Adobe Acrobat Reader DC Annotation Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1129: Magnet Forensics AXIOM Command Injection Remote Code Execution Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1128: Samsung MagicInfo Server getFileFromMultipartFile Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1127: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1126: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1125: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 13 Aug 2024

ZDI-24-1124: Foxit PDF Reader Doc Object Use-After-Free Information Disclosure Vulnerability

- Link

—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Wieder mal die Lieferkette: polyfill.io wird verkauft, spielt Schadcode aus.

Zum Youtube Video

6 Cyberangriffe: (Aug)

Datum	Opfer	Land	Information
2024-08-14	Flint	[USA]	Link
2024-08-13	District scolaire indépendant de Gadsden	[USA]	Link
2024-08-12	Benson, Kearley & Associates Insurance Brokers Ltd.	[CAN]	Link
2024-08-11	Université Paris-Saclay	[FRA]	Link
2024-08-11	AutoCanada	[CAN]	Link
2024-08-10	2Park	[NLD]	Link
2024-08-09	Quálitas	[MEX]	Link
2024-08-09	Schlatter Industries AG	[CHE]	Link
2024-08-08	Ohio School Boards Association (OSBA)	[USA]	Link
2024-08-08	Evolution Mining	[AUS]	Link
2024-08-07	Killeen	[USA]	Link
2024-08-06	Nilörn	[SWE]	Link
2024-08-06	Sumter County Sheriff's Office	[USA]	Link
2024-08-05	La ville de North Miami	[USA]	Link
2024-08-05	McLaren Health Care	[USA]	Link
2024-08-04	RMN-Grand Palais	[FRA]	Link
2024-08-03	Xtrim	[ECU]	Link
2024-08-02	Ihecs	[BEL]	Link

7 Ransomware-Erpressungen: (Aug)

Datum	Opfer	Ransomware-Grupppe	Webseite

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.