Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240818

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	0.990710000	Link
CVE-2023-5360	0.902780000	0.988750000	Link
CVE-2023-52251	0.944080000	0.992540000	Link
CVE-2023-4966	0.971280000	0.998290000	Link
CVE-2023-49103	0.962110000	0.995590000	Link
CVE-2023-48795	0.965330000	0.996440000	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	0.998620000	Link
CVE-2023-43177	0.964550000	0.996180000	Link
CVE-2023-42793	0.969020000	0.997460000	Link
CVE-2023-41265	0.911110000	0.989290000	Link
CVE-2023-39143	0.939130000	0.991960000	Link
CVE-2023-38646	0.906610000	0.988980000	Link
CVE-2023-38205	0.953670000	0.994100000	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	0.990800000	Link
CVE-2023-34634	0.925130000	0.990470000	Link
CVE-2023-34468	0.906650000	0.988990000	Link
CVE-2023-34362	0.971000000	0.998170000	Link
CVE-2023-34039	0.947770000	0.993080000	Link
CVE-2023-3368	0.932420000	0.991260000	Link
CVE-2023-33246	0.972040000	0.998510000	Link
CVE-2023-32315	0.970220000	0.997890000	Link
CVE-2023-30625	0.953800000	0.994120000	Link
CVE-2023-30013	0.962380000	0.995650000	Link
CVE-2023-29300	0.968930000	0.997440000	Link
CVE-2023-29298	0.947600000	0.993060000	Link
CVE-2023-28432	0.906190000	0.988940000	Link
CVE-2023-28343	0.942300000	0.992330000	Link
CVE-2023-28121	0.909500000	0.989150000	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	0.994550000	Link
CVE-2023-26360	0.965230000	0.996390000	Link
CVE-2023-26035	0.967360000	0.996990000	Link
CVE-2023-25717	0.954250000	0.994210000	Link
CVE-2023-25194	0.967920000	0.997150000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963740000	0.995960000	Link
CVE-2023-24489	0.973870000	0.999300000	Link
CVE-2023-23752	0.956380000	0.994600000	Link
CVE-2023-23333	0.962300000	0.995630000	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	0.994350000	Link
CVE-2023-21554	0.952830000	0.993950000	Link
CVE-2023-20887	0.970670000	0.998030000	Link
CVE-2023-1671	0.962480000	0.995660000	Link
CVE-2023-0669	0.969760000	0.997730000	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
8/17/2024	[Amazon Linux 2 : emacs (ALAS-2024-2608)]	critical
8/17/2024	[Amazon Linux 2 : freeradius (ALAS-2024-2611)]	critical
8/17/2024	[Amazon Linux 2 : openssl (ALAS-2024-2604)]	critical
8/17/2024	[SUSE SLES15 Security Update : libqt5-qtbase (SUSE-SU-2024:2946-1)]	critical
8/17/2024	[Fedora 39 : httpd (2024-e83af0855e)]	critical
8/17/2024	[Amazon Linux 2 : gtk3 (ALAS-2024-2602)]	high
8/17/2024	[Amazon Linux 2 : kernel (ALAS-2024-2613)]	high
8/17/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.15-2024-048)]	high
8/17/2024	[Amazon Linux 2 : openssl11 (ALAS-2024-2605)]	high
8/17/2024	[Amazon Linux 2 : ca-certificates (ALAS-2024-2607)]	high
8/17/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.15-2024-049)]	high
8/17/2024	[Amazon Linux 2 : tomcat (ALASTOMCAT9-2024-014)]	high
8/17/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.4-2024-077)]	high
8/17/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.10-2024-065)]	high
8/17/2024	[Amazon Linux 2 : gtk2 (ALAS-2024-2603)]	high

Datum	Schwachstelle	Bewertung
8/17/2024	[Amazon Linux 2 : tomcat (ALASTOMCAT8.5-2024-020)]	high
8/17/2024	[Amazon Linux 2 : bind (ALAS-2024-2616)]	high
8/17/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.4-2024-079)]	high
8/17/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.15-2024-050)]	high
8/17/2024	[Amazon Linux 2 : thunderbird (ALAS-2024-2617)]	high
8/17/2024	[SUSE SLES15 Security Update : kernel (SUSE-SU-2024:2948-1)]	high
8/17/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2024:2939-1)]	high
8/17/2024	[SUSE SLED12 / SLES12 Security Update : kernel (SUSE-SU-2024:2940-1)]	high
8/17/2024	[SUSE SLES12 Security Update : ucode-intel (SUSE-SU-2024:2941-1)]	high
8/17/2024	[SUSE SLES15 Security Update : kernel-firmware (SUSE-SU-2024:2944-1)]	high
8/17/2024	[SUSE SLES12 Security Update : python36-setuptools (SUSE-SU-2024:2950-1)]	high
8/17/2024	[Photon OS 4.0: Postgresql13 PHSA-2024-4.0-0667]	high
8/17/2024	[Photon OS 4.0: Go PHSA-2024-4.0-0668]	high
8/17/2024	[Photon OS 4.0: Postgresql14 PHSA-2024-4.0-0667]	high
8/17/2024	[Fedora 39 : bind / bind-dyndb-ldap (2024-ef8a7031e7)]	high
8/17/2024	[F5 Networks BIG-IP : BIND vulnerability (K000140732)]	high
8/17/2024	[openSUSE 15 Security Update : apptainer (openSUSE-SU-2024:0244-1)]	high
8/17/2024	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2024:2947-1)]	high
8/17/2024	[SUSE SLES15 Security Update : kernel-firmware (SUSE-SU-2024:2943-1)]	high
8/17/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.10-2024-066)]	high

Datum	Schwachstelle	Bewertung
8/17/2024	[FreeBSD : Dovecot – DoS (6a6ad6cb-5c6c-11ef-b456-001e676bf734)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Fri, 16 Aug 2024

WordPress Shield Security 20.0.5 Cross Site Scripting

WordPress Shield Security plugin versions 20.0.5 and below cross site scripting exploit that adds an administrative user.

- Link

—

” “Fri, 16 Aug 2024

Build Your Own Botnet 2.0.0 Remote Code Execution

Build Your Own Botnet (BYOB) version 2.0.0 exploit that works by spoofing an agent callback to overwrite the sqlite database and bypass authentication and exploiting an authenticated command injection in the payload builder page.

- Link

—

” “Fri, 16 Aug 2024

Insurance 1.2 Insecure Settings

Insurance version 1.2 suffers from an ignored default credential vulnerability.

- Link

—

” “Fri, 16 Aug 2024

Human Resource Management System 2024 1.0 SQL Injection

Human Resource Management System 2024 version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Fri, 16 Aug 2024

Hotel Management System 1.0 SQL Injection

Hotel Management System version 1.0 suffers from a remote SQL injection vulnerability that allows

for authentication bypass.

- Link

—

” “Fri, 16 Aug 2024

Hotel Booking System 1.0 Shell Upload

Hotel Booking System version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Fri, 16 Aug 2024

Home Owners Collection Management System 1.0 Insecure Settings

Home Owners Collection Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Fri, 16 Aug 2024

Giftora 1.0 Cross Site Scripting

Giftora version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Fri, 16 Aug 2024

Bhojon Restaurant Management System 3.0 Insecure Direct Object Reference

Bhojon Restaurant Management System version 3.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “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

—

”

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

—

”

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
2024-08-17	[TELECO]	stormous	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-17	[peoplewell.com]	darkvault	Link
2024-08-17	[aerworldwide.com]	lockbit3	Link
2024-08-17	[awsag.com]	madliberator	Link
2024-08-17	[www.albynhousing.org.uk]	ransomhub	Link
2024-08-17	[www.lennartsfors.com]	ransomhub	Link
2024-08-17	[www.allanmcneill.co.nz]	ransomhub	Link
2024-08-17	[www.martinswood.herts.sch.uk]	ransomhub	Link
2024-08-17	[www.gmchc.org]	ransomhub	Link
2024-08-17	[www.regentcaravans.com.au]	ransomhub	Link
2024-08-17	[www.netconfig.co.za]	ransomhub	Link
2024-08-17	[www.manotherm.ie]	ransomhub	Link
2024-08-17	[tiendasmacuto.com]	BrainCipher	Link
2024-08-15	[nrcollecties.nl]	ransomhub	Link
2024-08-17	[Zyxel.eu]	helldown	Link
2024-08-10	[www.wmwmeyer.com]	ransomhub	Link
2024-08-16	[www.vinakom.com]	ransomhub	Link
2024-08-16	[Keios Development Consulting]	ciphbit	Link
2024-08-16	[Lennartsfors AB]	meow	Link
2024-08-16	[Rostance Edwards]	meow	Link
2024-08-16	[SuperDrob S.A.]	hunters	Link
2024-08-16	[Sterling Rope]	rhysida	Link
2024-08-16	[www.patelco.org]	ransomhub	Link
2024-08-14	[ljglaw.com]	ransomhub	Link
2024-08-16	[Hiesmayr Haustechnik]	qilin	Link
2024-08-15	[www.aaconsultinc.com]	ransomhub	Link
2024-08-16	[promises2kids.org]	qilin	Link
2024-08-16	[BTS Biogas]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-15	[www.isnart.it]	ransomhub	Link
2024-08-15	[www.atwoodcherny.com]	ransomhub	Link
2024-08-13	[Mill Creek Lumber]	play	Link
2024-08-14	[Patterson Health Center]	qilin	Link
2024-08-15	[www.prinsotel.com]	qilin	Link
2024-08-15	[Seaway Manufacturing Corp.]	fog	Link
2024-08-15	[FD S.R.L]	ciphbit	Link
2024-08-15	[The Pyle Group]	medusa	Link
2024-08-15	[Zydus Pharmaceuticals]	meow	Link
2024-08-15	[EPS Tech Ltd]	handala	Link
2024-08-15	[MBS Radio]	metaencryptor	Link
2024-08-15	[Liberty Resources]	rhysida	Link
2024-08-15	[megatravel.com.mx]	darkvault	Link
2024-08-14	[startaxi.com]	killsec	Link
2024-08-14	[Boni]	akira	Link
2024-08-14	[The Washington Times]	rhysida	Link
2024-08-12	[Benson Kearley IFG - Insurance Brokers & Financial Advisors]	bianlian	Link
2024-08-14	[Texas Centers for Infectious Disease Associates]	bianlian	Link
2024-08-14	[Thompson Davis & Co]	bianlian	Link
2024-08-14	[police.praca.gov.pl]	ransomhub	Link
2024-08-14	[mmtransport.com]	dAn0n	Link
2024-08-14	[Riley Pope & Laney]	cicada3301	Link
2024-08-13	[hugwi.ch]	helldown	Link
2024-08-13	[Forrec]	blacksuit	Link
2024-08-13	[American Contract Systems]	meow	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-13	[Element Food Solutions]	meow	Link
2024-08-13	[Aerotech Solutions]	meow	Link
2024-08-13	[E-Z UP]	meow	Link
2024-08-13	[Safefood]	meow	Link
2024-08-13	[Gaston Fence]	meow	Link
2024-08-13	[Parker Development Company]	play	Link
2024-08-13	[Air International Thermal Systems]	play	Link
2024-08-13	[Adina Design]	play	Link
2024-08-13	[CinemaTech]	play	Link
2024-08-13	[Erie Meats]	play	Link
2024-08-13	[M??? ????k ??????]	play	Link
2024-08-13	[SCHLATTNER.de]	helldown	Link
2024-08-13	[deganis.fr]	helldown	Link
2024-08-13	[The White Center Community Development Association]	rhysida	Link
2024-08-13	[lenmed.co.za]	darkvault	Link
2024-08-13	[gpf.org.za]	darkvault	Link
2024-08-13	[Banner and Associates]	trinity	Link
2024-08-13	[Southwest Family Medicine Associates]	bianlian	Link
2024-08-13	[glazkov.co.il]	darkvault	Link
2024-08-05	[XPERT Business Solutions GmbH]	helldown	Link
2024-08-05	[MyFreightWorld]	helldown	Link
2024-08-09	[cbmm.org]	helldown	Link
2024-08-10	[AZIENDA TRASPORTI PUBBLICI S.P.A.]	helldown	Link
2024-08-11	[briju.pl]	helldown	Link
2024-08-11	[vindix.pl]	helldown	Link
2024-08-11	[Albatros S.r.l.]	helldown	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-12	[NetOne]	hunters	Link
2024-08-12	[fabamaq.com]	BrainCipher	Link
2024-08-12	[cyceron.fr]	BrainCipher	Link
2024-08-12	[bedford.k12.oh.us]	ransomhub	Link
2024-08-12	[Warwick Hotels and Resorts]	lynx	Link
2024-08-12	[VVS-Eksperten]	cicada3301	Link
2024-08-12	[Brookshire Dental]	qilin	Link
2024-08-07	[Alvan Blanch Development]	lynx	Link
2024-08-11	[parkerdevco.com]	dispossessor	Link
2024-08-11	[naturalcuriosities.com]	ransomhub	Link
2024-08-11	[TelPro]	play	Link
2024-08-11	[Jeffersoncountyclerk.org]	ransomhub	Link
2024-08-11	[Amco Metal Industrial Corporation]	qilin	Link
2024-08-11	[brockington.leisc.sch.uk]	lockbit3	Link
2024-08-11	[Moser Wealth Advisors]	rhysida	Link
2024-08-09	[alliuminteriors.co.nz]	ransomhub	Link
2024-08-11	[robertshvac.com]	abyss	Link
2024-08-11	[dmmerch.com]	lockbit3	Link
2024-08-11	[luisoliveras.com]	lockbit3	Link
2024-08-11	[legacycpas.com]	lockbit3	Link
2024-08-11	[allweatheraa.com]	lockbit3	Link
2024-08-11	[soprema.com]	lockbit3	Link
2024-08-11	[exol-lubricants.com]	lockbit3	Link
2024-08-11	[fremontschools.net]	lockbit3	Link
2024-08-11	[acdcexpress.com]	lockbit3	Link
2024-08-11	[clinicatezza.com.pe]	lockbit3	Link
2024-08-11	[divaris.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-11	[sullivansteelservice.com]	lockbit3	Link
2024-08-11	[johnllowery.com]	lockbit3	Link
2024-08-11	[qespavements.com]	lockbit3	Link
2024-08-11	[emanic.net]	lockbit3	Link
2024-08-11	[Hanon Systems]	hunters	Link
2024-08-10	[kronospublic.com]	lockbit3	Link
2024-08-10	[Brontoo Technology Solutions]	ransomexx	Link
2024-08-07	[Cydcor]	dragonforce	Link
2024-08-09	[Credible Group]	play	Link
2024-08-09	[Nilorngruppen AB]	play	Link
2024-08-09	[www.arkworkplacerisk.co.uk]	alphalocker	Link
2024-08-09	[Anniversary Holding Company]	bianlian	Link
2024-08-09	[GCA Global Cargo Alliance]	bianlian	Link
2024-08-09	[Majestic Metals]	bianlian	Link
2024-08-09	[dhcgrp.com]	ransomhub	Link
2024-08-05	[Boombah Inc.]	incransom	Link
2024-08-09	[www.dunnsolutions.com]	dAn0n	Link
2024-08-09	[Sumter County Sheriff]	rhysida	Link
2024-08-06	[pierrediamonds.com.au]	ransomhub	Link
2024-08-08	[golfoy.com]	ransomhub	Link
2024-08-08	[inv-dar.com]	ransomhub	Link
2024-08-08	[icarasia.com]	killsec	Link
2024-08-08	[rationalenterprise.com]	ransomhub	Link
2024-08-02	[modernceramics.com]	ransomhub	Link
2024-08-08	[goftac.com/ firsttx.com First Texas Alliance Corp (FTAC)]	alphalocker	Link
2024-08-08	[tibaitservices.com]	cactus	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-08	[mihlfeld.com]	cactus	Link
2024-08-08	[Horizon View Medical Center]	everest	Link
2024-08-08	[comoferta.com]	darkvault	Link
2024-08-08	[NIDEC CORPORATION]	everest	Link
2024-08-08	[mercadomineiro.com.br]	darkvault	Link
2024-08-07	[hudsoncivil.com.au]	ransomhub	Link
2024-08-07	[www.jgsummit.com.ph]	ransomhub	Link
2024-08-07	[Bayhealth Hospital]	rhysida	Link
2024-08-07	[amplicon.com]	ransomhub	Link
2024-08-06	[infotexim.pe]	ransomhub	Link
2024-08-07	[suandco.com]	madliberator	Link
2024-08-07	[Anderson Oil & Gas]	hunters	Link
2024-08-07	[bonatra.com]	killsec	Link
2024-08-07	[FatBoy Cellular]	meow	Link
2024-08-07	[KLA]	meow	Link
2024-08-07	[HUD User]	meow	Link
2024-08-06	[msprocuradores.es]	madliberator	Link
2024-08-06	[www.carri.com]	alphalocker	Link
2024-08-06	[www.consorzioinnova.it]	alphalocker	Link
2024-08-06	[goftac.com/ firsttx.com First Texas Alliance Corp (FTAC)]	alphalocker	Link
2024-08-06	[biw-burger.de]	alphalocker	Link
2024-08-06	[www.sobha.com]	ransomhub	Link
2024-08-06	[Alternate Energy]	play	Link
2024-08-06	[True Blue Environmental]	play	Link
2024-08-06	[Granit Design]	play	Link
2024-08-06	[KinetX]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-06	[Omni Family Health]	hunters	Link
2024-08-06	[IOI Corporation Berhad]	fog	Link
2024-08-06	[Ziba Design]	fog	Link
2024-08-06	[Casco Antiguo]	hunters	Link
2024-08-06	[Fractalia Group]	hunters	Link
2024-08-06	[Banx Systems]	meow	Link
2024-08-05	[Silipos]	cicada3301	Link
2024-08-04	[kierlcpa.com]	lockbit3	Link
2024-08-05	[Square One Coating Systems]	cicada3301	Link
2024-08-05	[Hi-P International]	fog	Link
2024-08-05	[Zon Beachside zonbeachside.com]	dispossessor	Link
2024-08-05	[HP Distribution]	incransom	Link
2024-08-05	[exco-solutions.com]	cactus	Link
2024-08-05	[Maryville Academy]	rhysida	Link
2024-08-04	[notariusze.waw.pl]	killsec	Link
2024-08-04	[Ranney School]	rhysida	Link
2024-08-03	[nursing.com]	ransomexx	Link
2024-08-03	[Bettis Asphalt]	blacksuit	Link
2024-08-03	[fcl.crs]	lockbit3	Link
2024-08-03	[CPA Tax Solutions]	meow	Link
2024-08-03	[LRN]	hunters	Link
2024-08-03	[aikenhousing.org]	blacksuit	Link
2024-08-02	[David E Shambach Architect]	dragonforce	Link
2024-08-02	[Hayes Beer Distributing]	dragonforce	Link
2024-08-02	[Jangho Group]	hunters	Link
2024-08-02	[Khandelwal Laboratories Pvt]	hunters	Link
2024-08-02	[retaildatallc.com]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-02	[WPG Holdings]	meow	Link
2024-08-02	[National Beverage]	meow	Link
2024-08-02	[PeoplesHR]	meow	Link
2024-08-02	[Dometic Group]	meow	Link
2024-08-02	[Remitano]	meow	Link
2024-08-02	[Premier Equities]	meow	Link
2024-08-01	[Kemlon Products & Development Co Inc]	spacebears	Link
2024-08-02	[q-cells.de]	abyss	Link
2024-08-02	[coinbv.nl]	madliberator	Link
2024-08-01	[Valley Bulk]	cicada3301	Link
2024-08-01	[ENEA Italy]	hunters	Link
2024-08-01	[mcdowallaffleck.com.au]	ransomhub	Link
2024-08-01	[effinghamschools.com]	ransomhub	Link
2024-08-01	[warrendale-wagyu.co.uk]	darkvault	Link
2024-08-01	[Adorna & Guzman Dentistry]	monti	Link
2024-08-01	[Camp Susque]	medusa	Link
2024-08-01	[Ali Gohar]	medusa	Link
2024-08-01	[acsi.org]	blacksuit	Link
2024-08-01	[County Linen UK]	dispossessor	Link
2024-08-01	[TNT Materials tnt-materials.com/]	dispossessor	Link
2024-08-01	[Peñoles]	akira	Link
2024-08-01	[dahlvalve.com]	cactus	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.