

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240812



## Inhaltsverzeichnis

<b>1 Editorial</b>	<b>2</b>
<b>2 Security-News</b>	<b>3</b>
2.1 Heise - Security-Alert . . . . .	3
<b>3 Sicherheitslücken</b>	<b>4</b>
3.1 EPSS . . . . .	4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit . . . . .	5
3.2 BSI - Warn- und Informationsdienst (WID) . . . . .	7
3.3 Sicherheitslücken Meldungen von Tenable . . . . .	11
<b>4 Aktiv ausgenutzte Sicherheitslücken</b>	<b>12</b>
4.1 Exploits der letzten 5 Tage . . . . .	12
4.2 0-Days der letzten 5 Tage . . . . .	17
<b>5 Die Hacks der Woche</b>	<b>20</b>
5.0.1 Wieder mal die Lieferkette: polyfill.io wird verkauft, spielt Schadcode aus. . . .	20
<b>6 Cyberangriffe: (Aug)</b>	<b>21</b>
<b>7 Ransomware-Erpressungen: (Aug)</b>	<b>21</b>
<b>8 Quellen</b>	<b>26</b>
8.1 Quellenverzeichnis . . . . .	26
<b>9 Impressum</b>	<b>27</b>

## 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

#### ***CPU-Sicherheitslücke in AMD-Prozessoren ermöglicht Malware-Infektionen***

Sicherheitsforscher haben eine als Sinkclose bezeichnete Sicherheitslücke in AMD-CPU's entdeckt und auf der Defcon 32 in Las Vegas präsentiert.

- [Link](#)

—

#### ***Sicherheitstipps Cisco: Angreifer missbrauchen Smart-Install-Protokoll***

Ein Dienst zur Fernkonfiguration für Switches von Cisco und schwache Passwörter spielen Angreifer in die Karten. Doch dagegen können Admins etwas machen.

- [Link](#)

—

#### ***Attacken auf Android-Kernel, Apache OfBiz und Progress WhatsUp***

Auf Sicherheitslücken im Android-Kernel, Apache OfBiz und Progress WhatsUp finden inzwischen Angriffe in freier Wildbahn statt.

- [Link](#)

—

#### ***Roundcube Webmail: Angreifer können durch kritische Lücke E-Mails kapern***

Admins sollten Roundcube aus Sicherheitsgründen auf den aktuellen Stand bringen. Viele Universitäten setzen auf dieses Webmailprodukt.

- [Link](#)

—

#### ***Cisco: Angreifer können Befehle auf IP-Telefonen ausführen, Update kommt nicht***

Für kritische Lücken in Cisco-IP-Telefonen wird es keine Updates geben. Für eine jüngst gemeldete Lücke ist ein Proof-of-Concept-Exploit aufgetaucht.

- [Link](#)

—

#### ***TeamCity: Fehlerhafte Rechtevergabe ermöglicht Rechteauserweiterung***

Eine Sicherheitslücke in TeamCity ermöglicht Angreifern, ihre Rechte auszuweiten. Ein bereitstehendes Update korrigiert den Fehler.

- [Link](#)

—

#### ***Mail-Client und Webbrowser: Chrome, Firefox und Thunderbird attackierbar***

Angreifer können an mehreren Sicherheitslücken in Chrome, Firefox und Thunderbird ansetzen. Mittlerweile wurden die Lücken geschlossen.

- [Link](#)

---

***Sicherheitsupdate: Kritische Schadcode-Lücke bedroht Analyseplattform Kibana***

In aktuellen Versionen haben die Kibana-Entwickler ein gefährliches Sicherheitsproblem gelöst.

- [Link](#)

---

***Patchday: Attacken auf Android-Geräte beobachtet***

Google hat mehrere Schwachstellen in seinem mobilen Betriebssystem Android geschlossen.

- [Link](#)

---

***E-Book-Tool Calibre: Codeschmuggel durch kritische Sicherheitslücke möglich***

Durch eine kritische Sicherheitslücke im E-Book-Tool Calibre können nicht angemeldete Angreifer Code einschleusen. Ein Update dichtet das Leck ab.

- [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	0.903160000	0.988710000	<a href="#">Link</a>
CVE-2023-6895	0.922010000	0.990050000	<a href="#">Link</a>
CVE-2023-6553	0.925190000	0.990450000	<a href="#">Link</a>
CVE-2023-5360	0.903980000	0.988760000	<a href="#">Link</a>
CVE-2023-52251	0.944080000	0.992550000	<a href="#">Link</a>
CVE-2023-4966	0.971280000	0.998330000	<a href="#">Link</a>
CVE-2023-49103	0.962110000	0.995600000	<a href="#">Link</a>
CVE-2023-48795	0.964660000	0.996190000	<a href="#">Link</a>
CVE-2023-47246	0.953860000	0.994150000	<a href="#">Link</a>
CVE-2023-46805	0.937250000	0.991710000	<a href="#">Link</a>
CVE-2023-46747	0.972820000	0.998900000	<a href="#">Link</a>
CVE-2023-46604	0.961790000	0.995530000	<a href="#">Link</a>
CVE-2023-4542	0.928310000	0.990760000	<a href="#">Link</a>
CVE-2023-43208	0.966400000	0.996700000	<a href="#">Link</a>
CVE-2023-43177	0.964550000	0.996170000	<a href="#">Link</a>
CVE-2023-42793	0.969020000	0.997480000	<a href="#">Link</a>
CVE-2023-41265	0.911110000	0.989280000	<a href="#">Link</a>
CVE-2023-39143	0.939130000	0.991950000	<a href="#">Link</a>
CVE-2023-38646	0.906610000	0.988960000	<a href="#">Link</a>
CVE-2023-38205	0.947910000	0.993120000	<a href="#">Link</a>
CVE-2023-38203	0.966410000	0.996710000	<a href="#">Link</a>
CVE-2023-38035	0.974680000	0.999710000	<a href="#">Link</a>
CVE-2023-36845	0.964250000	0.996100000	<a href="#">Link</a>
CVE-2023-3519	0.965340000	0.996430000	<a href="#">Link</a>
CVE-2023-35082	0.966130000	0.996630000	<a href="#">Link</a>
CVE-2023-35078	0.970390000	0.997950000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34993	0.972640000	0.998810000	<a href="#">Link</a>
CVE-2023-34960	0.928290000	0.990760000	<a href="#">Link</a>
CVE-2023-34634	0.925130000	0.990440000	<a href="#">Link</a>
CVE-2023-34468	0.906650000	0.988970000	<a href="#">Link</a>
CVE-2023-34362	0.971000000	0.998200000	<a href="#">Link</a>
CVE-2023-34039	0.947770000	0.993070000	<a href="#">Link</a>
CVE-2023-3368	0.932420000	0.991240000	<a href="#">Link</a>
CVE-2023-33246	0.972140000	0.998620000	<a href="#">Link</a>
CVE-2023-32315	0.970550000	0.998010000	<a href="#">Link</a>
CVE-2023-30625	0.948260000	0.993190000	<a href="#">Link</a>
CVE-2023-30013	0.962380000	0.995660000	<a href="#">Link</a>
CVE-2023-29300	0.968930000	0.997450000	<a href="#">Link</a>
CVE-2023-29298	0.943640000	0.992510000	<a href="#">Link</a>
CVE-2023-28432	0.906190000	0.988930000	<a href="#">Link</a>
CVE-2023-28343	0.942300000	0.992330000	<a href="#">Link</a>
CVE-2023-28121	0.909500000	0.989140000	<a href="#">Link</a>
CVE-2023-27524	0.970600000	0.998030000	<a href="#">Link</a>
CVE-2023-27372	0.972120000	0.998610000	<a href="#">Link</a>
CVE-2023-27350	0.969720000	0.997740000	<a href="#">Link</a>
CVE-2023-26469	0.953920000	0.994170000	<a href="#">Link</a>
CVE-2023-26360	0.965230000	0.996380000	<a href="#">Link</a>
CVE-2023-26035	0.967360000	0.996990000	<a href="#">Link</a>
CVE-2023-25717	0.954250000	0.994240000	<a href="#">Link</a>
CVE-2023-25194	0.968820000	0.997430000	<a href="#">Link</a>
CVE-2023-2479	0.963740000	0.995970000	<a href="#">Link</a>
CVE-2023-24489	0.973870000	0.999310000	<a href="#">Link</a>
CVE-2023-23752	0.956380000	0.994630000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23333	0.958950000	0.994990000	<a href="#">Link</a>
CVE-2023-22527	0.968290000	0.997270000	<a href="#">Link</a>
CVE-2023-22518	0.964890000	0.996230000	<a href="#">Link</a>
CVE-2023-22515	0.973250000	0.999060000	<a href="#">Link</a>
CVE-2023-21839	0.955020000	0.994380000	<a href="#">Link</a>
CVE-2023-21554	0.952830000	0.993950000	<a href="#">Link</a>
CVE-2023-20887	0.970670000	0.998050000	<a href="#">Link</a>
CVE-2023-1671	0.962480000	0.995670000	<a href="#">Link</a>
CVE-2023-0669	0.969440000	0.997630000	<a href="#">Link</a>

### 3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 09 Aug 2024

**[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht Codeausführung**

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

- [Link](#)

—

Fri, 09 Aug 2024

**[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht Denial of Service**

Ein lokaler Angreifer kann eine Schwachstelle in QEMU ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Fri, 09 Aug 2024

**[UPDATE] [hoch] Xerox FreeFlow Print Server: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Xerox FreeFlow Print Server ausnutzen, um die Vertraulichkeit, Verfügbarkeit und Integrität des Systems zu gefährden.

- [Link](#)

—



Fri, 09 Aug 2024

**[UPDATE] [hoch] ffmpeg: Mehrere Schwachstellen**

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

- [Link](#)

—

Fri, 09 Aug 2024

**[NEU] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in PostgreSQL ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Fri, 09 Aug 2024

**[NEU] [hoch] Microsoft Edge: Mehrere Schwachstellen ermöglichen Codeausführung**

Ein Angreifer kann mehrere Schwachstellen in Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 09 Aug 2024

**[NEU] [hoch] IBM Business Automation Workflow: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in IBM Business Automation Workflow ausnutzen, um Informationen offenzulegen oder beliebigen Code auszuführen.

- [Link](#)

—

Fri, 09 Aug 2024

**[UPDATE] [hoch] SaltStack Salt: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in SaltStack Salt ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen und die Authentisierung zu umgehen.

- [Link](#)

—

Fri, 09 Aug 2024

**[UPDATE] [hoch] SaltStack Salt: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in SaltStack Salt ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 09 Aug 2024

**[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht nicht spezifizierten Angriff**

Ein Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Fri, 09 Aug 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](#)

—

Fri, 09 Aug 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](#)

—

Fri, 09 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](#)

—

Fri, 09 Aug 2024

**[UPDATE] [kritisch] Microsoft Windows: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in verschiedenen Versionen von Microsoft Windows und Microsoft Windows Server ausnutzen, um seine Privilegien zu erweitern, beliebigen Programmcode auszuführen, Informationen offenzulegen, Dateien zu manipulieren oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Fri, 09 Aug 2024

**[UPDATE] [hoch] Red Hat Enterprise Linux (python-setuptools): Schwachstelle ermöglicht Codeausführung**

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

- [Link](#)

—

Fri, 09 Aug 2024

**[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen**

Ein entfernter anonymen Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Code auszuführen oder einen unspezifischen Angriff durchzuführen.

- [Link](#)

—

Fri, 09 Aug 2024

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

Ein entfernter anonymen 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](#)

—

Thu, 08 Aug 2024

**[NEU] [UNGEPATCHT] [kritisch] Cisco IP Phone: Mehrere Schwachstellen**

Ein entfernter anonymen Angreifer kann mehrere Schwachstellen in Cisco IP Phone ausnutzen, um beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Thu, 08 Aug 2024

**[NEU] [hoch] Jenkins: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in Jenkins ausnutzen, um beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Thu, 08 Aug 2024

**[NEU] [hoch] Poly Clariti: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in Poly Clariti ausnutzen, um einen Cross-Site-Scripting-Angriff zu starten, um Sicherheitsmaßnahmen zu umgehen oder um beliebigen Code auszuführen.

- [Link](#)

—

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/9/2024	[Cisco Smart Software Manager On-Prem Password Change (cisco-sa-cssm-auth-sLw3uhUy)]	critical
8/11/2024	[GLSA-202408-24 : Ruby on Rails: Remote Code Execution]	critical
8/11/2024	[GLSA-202408-27 : AFLplusplus: Arbitrary Code Execution]	critical
8/10/2024	[GLSA-202408-20 : libde265: Multiple Vulnerabilities]	critical
8/10/2024	[GLSA-202408-21 : GPAC: Multiple Vulnerabilities]	critical
8/9/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-38583)]	high
8/9/2024	[FreeBSD : soft-serve – Remote code execution vulnerability (8c342a6c-563f-11ef-a77e-901b0e9408dc)]	high
8/9/2024	[Ubuntu 16.04 LTS : Linux kernel (Azure) vulnerabilities (USN-6926-3)]	high
8/9/2024	[Oracle Linux 8 : kernel (ELSA-2024-5101)]	high
8/9/2024	[Oracle Linux 7 : linux-firmware (ELSA-2024-12579)]	high
8/9/2024	[Rocket.Chat < 6.10.1 Server-Side Request Forgery]	high
8/11/2024	[Fedora 39 : python-setuptools (2024-9ed182a5d3)]	high
8/11/2024	[GLSA-202408-25 : runc: Multiple Vulnerabilities]	high
8/11/2024	[FreeBSD : AMD CPUs – Guest Memory Vulnerabilities (7d631146-5769-11ef-b618-1c697a616631)]	high
8/11/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2023-52340)]	high
8/11/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2022-48788)]	high
8/11/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-42072)]	high
8/11/2024	[GLSA-202408-26 : matio: Multiple Vulnerabilities]	high
8/11/2024	[GLSA-202408-28 : rsyslog: Heap Buffer Overflow]	high
8/10/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : bind (SUSE-SU-2024:2862-1)]	high
8/10/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : ca-certificates-mozilla (SUSE-SU-2024:2869-1)]	high

Datum	Schwachstelle	Bewertung
8/10/2024	[SUSE SLES15 Security Update : bind (SUSE-SU-2024:2863-1)]	high
8/10/2024	[SUSE SLES12 Security Update : bind (SUSE-SU-2024:2868-1)]	high
8/10/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : ffmpeg-4 (SUSE-SU-2024:2864-1)]	high
8/10/2024	[openSUSE 15 Security Update : python-Django (SUSE-SU-2024:2861-1)]	high
8/10/2024	[SUSE SLES15 / openSUSE 15 Security Update : python3-Twisted (SUSE-SU-2024:2860-1)]	high
8/10/2024	[GLSA-202408-22 : Bundler: Multiple Vulnerabilities]	high
8/10/2024	[CBL Mariner 2.0 Security Update: msft-golang / golang (CVE-2022-41722)]	high
8/10/2024	[FreeBSD : Roundcube – Multiple vulnerabilities (5776cc4f-5717-11ef-b611-84a93843eb75)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Fri, 09 Aug 2024

#### **Gaati Track 1.0-2023 Insecure Direct Object Reference**

Gaati Track version 1.0-2023 suffers from an insecure direct object reference vulnerability.

- [Link](#)

—

” “Fri, 09 Aug 2024

#### **Farmacia Gama 1.0 File Inclusion**

Farmacia Gama version 1.0 suffers from a file inclusion vulnerability.

- [Link](#)

—

” “Fri, 09 Aug 2024

#### **Employee Management System 1.0 Cross Site Request Forgery**

Employee Management System version 1.0 suffers from a cross site request forgery vulnerability.

- [Link](#)

—

” “Fri, 09 Aug 2024

***E-Commerce Site Using PHP PDO 1.0 Cross Site Scripting***

E-Commerce Site using PHP PDO version 1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Fri, 09 Aug 2024

***Bhojon Restaurant Management System 2.8 Insecure Direct Object Reference***

Bhojon Restaurant Management System version 2.9 suffers from an insecure direct object reference vulnerability.

- [Link](#)

—

” “Fri, 09 Aug 2024

***Xain-Hotel Management System 2.5 Insecure Settings***

Xain-Hotel Management System version 2.5 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Fri, 09 Aug 2024

***Yoga Class Registration System 1.0 Cross Site Request Forgery***

Yoga Class Registration System version 1.0 suffers from a cross site request forgery vulnerability.

- [Link](#)

—

” “Fri, 09 Aug 2024

***Exam Form Submission 1.0 Arbitrary File Upload***

Exam Form Submission version 1.0 suffers from an arbitrary file upload vulnerability.

- [Link](#)

—

” “Fri, 09 Aug 2024

***AccPack Khanepani 1.0 Arbitrary File Upload***

AccPack Khanepani version 1.0 suffers from an arbitrary file upload vulnerability.

- [Link](#)

—

” “Fri, 09 Aug 2024

***AccPack Cop 1.0 Arbitrary File Upload***

AccPack Cop version 1.0 suffers from an arbitrary file upload vulnerability.

- [Link](#)

—  
" "Thu, 08 Aug 2024

#### ***Calibre 7.15.0 Python Code Injection***

This Metasploit module exploits a Python code injection vulnerability in the Content Server component of Calibre version 6.9.0 through 7.15.0. Once enabled (disabled by default), it will listen in its default configuration on all network interfaces on TCP port 8080 for incoming traffic, and does not require any authentication. The injected payload will get executed in the same context under which Calibre is being executed.

- [Link](#)

—  
" "Thu, 08 Aug 2024

#### ***Journyx 11.5.4 XML Injection***

Journyx version 11.5.4 has an issue where the soap.cgi.pyc API handler allows the XML body of SOAP requests to contain references to external entities. This allows an unauthenticated attacker to read local files, perform server-side request forgery, and overwhelm the web server resources.

- [Link](#)

—  
" "Thu, 08 Aug 2024

#### ***Journyx 11.5.4 Cross Site Scripting***

Journyx version 11.5.4 suffers from a cross site scripting vulnerability due to mishandling of the error\_description during an active directory login flow.

- [Link](#)

—  
" "Thu, 08 Aug 2024

#### ***Journyx 11.5.4 Authenticated Remote Code Execution***

Journyx version 11.5.4 has an issue where attackers with a valid username and password can exploit a python code injection vulnerability during the natural login flow.

- [Link](#)

—  
" "Thu, 08 Aug 2024

#### ***Journyx 11.5.4 Unauthenticated Password Reset Bruteforce***

Journyx version 11.5.4 suffers from an issue where password reset tokens are generated using an insecure source of randomness. Attackers who know the username of the Journyx installation user can bruteforce the password reset and change the administrator password.

- [Link](#)

—  
" "Thu, 08 Aug 2024

#### ***Open WebUI 0.1.105 File Upload / Path Traversal***

Open WebUI version 0.1.105 suffers from arbitrary file upload and path traversal vulnerabilities.

- [Link](#)

—

” “Thu, 08 Aug 2024

#### ***Open WebUI 0.1.105 Persistent Cross Site Scripting***

Open WebUI version 0.1.105 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Thu, 08 Aug 2024

#### ***Oracle VM VirtualBox 7.0.10 r158379 Escape***

A guest inside a VirtualBox VM using the virtio-net network adapter can trigger an intra-object out-of-bounds write in src/VBox/Devices/Network/DevVirtioNet.cpp to cause a denial-of-service or escape the hypervisor and compromise the host. This is Google’s proof of concept exploit.

- [Link](#)

—

” “Thu, 08 Aug 2024

#### ***Linux eBPF Path Pruning Gone Wrong***

A bug in the eBPF Verifier branch pruning logic can lead to unsafe code paths being incorrectly marked as safe. As demonstrated in the exploitation section, this can be leveraged to get arbitrary read/write in kernel memory, leading to local privilege escalation and Container escape.

- [Link](#)

—

” “Thu, 08 Aug 2024

#### ***XGETBV Is Non-Deterministic On Intel CPUs***

The XGETBV instruction reads the contents of an internal control register. It is not a privileged instruction and is usually available to userspace. The contents is also exposed via the xstate\_bv header in the XSAVE structure. The primary use of XGETBV is determining the XINUSE flags, which allows kernels and userthread implementations to determine what CPU state needs to be saved or restored on context switch. However, it has been observed that these flags appear to be non-deterministic on various Intel CPUs. The data here is currently research and not necessarily considered a security issue, but a reproducer has been included.

- [Link](#)

—

” “Thu, 08 Aug 2024

#### ***XSAVES Instruction May Fail To Save XMM Registers***

AMD Errata 1386 1 is a flaw that affects the AMD Zen 2 family of processors. The observed result of this bug is that changes to xmm or ymm extended registers during normal program execution may be unexpectedly discarded. The implications of this flaw will vary depending on the workload. This is



Google's proof of concept exploit.

- [Link](#)

—

” “Thu, 08 Aug 2024

***RET2ASLR - Leaking ASLR From Return Instructions***

This is a proof of concept code from Google called RET2ASLR - Leaking ASLR from return instructions.

- [Link](#)

—

” “Thu, 08 Aug 2024

***Unexpected Speculation Control Of RETs***

Google observed some undocumented (to the best of their knowledge) behavior of the indirect branch predictors, specifically relative to *ret* instructions. The research they conducted appears to show that this behavior does not seem to create exploitable security vulnerabilities in the software they have tested. They would like to better understand the impact and implications for different software stacks, thus they welcome feedback or further research. Included is proof of concept code.

- [Link](#)

—

” “Thu, 08 Aug 2024

***Bleve Library Traversal***

This is a path traversal vulnerability that impacts the CreateIndexHandler and DeleteIndexHandler found within Bleve search library. These vulnerabilities enable the attacker to delete any directory owned by the user recursively, and create a new directory in any location which the server has write permissions to. This is Google's proof of concept exploit.

- [Link](#)

—

” “Thu, 08 Aug 2024

***Microsoft CBC Padding Oracle In Azure Blob Storage Encryption Library***

The Azure Storage Encryption library in Java and other languages is vulnerable to a CBC Padding Oracle attack, similar to CVE-2020-8911. The library is not vulnerable to the equivalent of CVE-2020-8912, but only because it currently only supports AES-CBC as encryption mode. This is Google's proof of concept exploit.

- [Link](#)

—

”

## 4.2 0-Days der letzten 5 Tage

“Thu, 08 Aug 2024

**ZDI-24-1122: Apple macOS VideoToolbox Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Thu, 08 Aug 2024

**ZDI-24-1121: Apple macOS VideoToolbox Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Thu, 08 Aug 2024

**ZDI-24-1120: Apple macOS AppleVADriver Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 08 Aug 2024

**ZDI-24-1119: Apple macOS AMDRadeonX6000MTLDriver KTX Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Thu, 08 Aug 2024

**ZDI-24-1118: Apple macOS AMDRadeonX6000MTLDriver KTX Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 08 Aug 2024

**ZDI-24-1117: Apple macOS AMDRadeonX6000MTLDriver KTX Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Thu, 08 Aug 2024

**ZDI-24-1116: Apple macOS AMDRadeonX6000MTLDriver KTX Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 08 Aug 2024

**ZDI-24-1115: Apple macOS AMDRadeonX6000MTLDriver KTX Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 08 Aug 2024

**ZDI-24-1114: Apple macOS AMDRadeonX6000MTLDriver KTX Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Thu, 08 Aug 2024

**ZDI-24-1113: Apple macOS AMDRadeonX6000MTLDriver KTX Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Thu, 08 Aug 2024

**ZDI-24-1112: Apple macOS AMDRadeonX6000MTLDriver KTX Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 08 Aug 2024

**ZDI-24-1111: Apple macOS AMDRadeonX6000MTLDriver KTX Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Thu, 08 Aug 2024

**ZDI-24-1110: Apple macOS AMDRadeonX6000MTLDriver KTX Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Thu, 08 Aug 2024

**ZDI-24-1109: Apple macOS AMDRadeonX6000MTLDriver KTX Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Thu, 08 Aug 2024

**ZDI-24-1108: Apple macOS AMDRadeonX6000MTLDriver KTX Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Thu, 08 Aug 2024

***ZDI-24-1107: Apple macOS AMDRadeonX6000MTLDriver KTX Parsing Out-Of-Bounds Read Information Disclosure Vulnerability***

- [Link](#)

—

” “Thu, 08 Aug 2024

***ZDI-24-1106: Logsign Unified SecOps Platform Directory data\_export\_delete\_all Traversal Arbitrary File Deletion Vulnerability***

- [Link](#)

—

” “Thu, 08 Aug 2024

***ZDI-24-1105: Logsign Unified SecOps Platform Directory Traversal Arbitrary Directory Deletion Vulnerability***

- [Link](#)

—

” “Thu, 08 Aug 2024

***ZDI-24-1104: Logsign Unified SecOps Platform Incorrect Authorization Authentication Bypass Vulnerability***

- [Link](#)

—

” “Thu, 08 Aug 2024

***ZDI-24-1103: Logsign Unified SecOps Platform Directory Traversal Arbitrary File Deletion Vulnerability***

- [Link](#)

—

” “Thu, 08 Aug 2024

***ZDI-24-1102: Logsign Unified SecOps Platform Directory Traversal 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
2024-08-10	2Park	[NLD]	<a href="#">Link</a>
2024-08-09	Quáalitas	[MEX]	<a href="#">Link</a>
2024-08-08	Ohio School Boards Association (OSBA)	[USA]	<a href="#">Link</a>
2024-08-07	Killeen	[USA]	<a href="#">Link</a>
2024-08-06	Nilörn	[SWE]	<a href="#">Link</a>
2024-08-06	Sumter County Sheriff's Office	[USA]	<a href="#">Link</a>
2024-08-05	La ville de North Miami	[USA]	<a href="#">Link</a>
2024-08-05	McLaren Health Care	[USA]	<a href="#">Link</a>
2024-08-04	RMN-Grand Palais	[FRA]	<a href="#">Link</a>
2024-08-03	Xtrim	[ECU]	<a href="#">Link</a>
2024-08-02	Ihecs	[BEL]	<a href="#">Link</a>

## 7 Ransomware-Erpressungen: (Aug)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-07	[Alvan Blanch Development]	lynx	<a href="#">Link</a>
2024-08-11	[parkerdevco.com]	dispossessor	<a href="#">Link</a>
2024-08-11	[naturalcuriosities.com]	ransomhub	<a href="#">Link</a>
2024-08-11	[TelPro]	play	<a href="#">Link</a>
2024-08-11	[Jeffersoncountyclerk.org]	ransomhub	<a href="#">Link</a>
2024-08-11	[Amco Metal Industrial Corporation]	qilin	<a href="#">Link</a>
2024-08-11	[brockington.leisc.sch.uk]	lockbit3	<a href="#">Link</a>
2024-08-11	[Moser Wealth Advisors]	rhysida	<a href="#">Link</a>
2024-08-09	[alliuminteriors.co.nz]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-11	[robertshvac.com]	abyss	<a href="#">Link</a>
2024-08-11	[dmmerch.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[luisoliveras.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[legacypas.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[allweatheraa.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[soprema.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[exol-lubricants.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[fremontschools.net]	lockbit3	<a href="#">Link</a>
2024-08-11	[acdexpress.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[clinatezza.com.pe]	lockbit3	<a href="#">Link</a>
2024-08-11	[divaris.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[sullivansteelservice.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[johnllowery.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[qespavements.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[emanic.net]	lockbit3	<a href="#">Link</a>
2024-08-11	[Hanon Systems]	hunters	<a href="#">Link</a>
2024-08-10	[kronospublic.com]	lockbit3	<a href="#">Link</a>
2024-08-10	[Brontoo Technology Solutions]	ransomexx	<a href="#">Link</a>
2024-08-07	[Cydcor]	dragonforce	<a href="#">Link</a>
2024-08-09	[Credible Group]	play	<a href="#">Link</a>
2024-08-09	[Nilorgruppen AB]	play	<a href="#">Link</a>
2024-08-09	[www.arkworkplacerisk.co.uk]	alphalocker	<a href="#">Link</a>
2024-08-09	[Anniversary Holding Company]	bianlian	<a href="#">Link</a>
2024-08-09	[GCA Global Cargo Alliance]	bianlian	<a href="#">Link</a>
2024-08-09	[Majestic Metals]	bianlian	<a href="#">Link</a>
2024-08-09	[dhcgrp.com]	ransomhub	<a href="#">Link</a>
2024-08-05	[Boombah Inc.]	incransom	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-09	[www.dunnsolutions.com]	dAn0n	<a href="#">Link</a>
2024-08-09	[Sumter County Sheriff]	rhysida	<a href="#">Link</a>
2024-08-06	[pierrediamonds.com.au]	ransomhub	<a href="#">Link</a>
2024-08-08	[golfoy.com]	ransomhub	<a href="#">Link</a>
2024-08-08	[inv-dar.com]	ransomhub	<a href="#">Link</a>
2024-08-08	[icarasia.com]	killsec	<a href="#">Link</a>
2024-08-08	[rationalenterprise.com]	ransomhub	<a href="#">Link</a>
2024-08-02	[modernceramics.com]	ransomhub	<a href="#">Link</a>
2024-08-08	[goftac.com/ firsttx.com First Texas Alliance Corp (FTAC)]	alphalocker	<a href="#">Link</a>
2024-08-08	[tibaitservices.com]	cactus	<a href="#">Link</a>
2024-08-08	[mihlfeld.com]	cactus	<a href="#">Link</a>
2024-08-08	[Horizon View Medical Center]	everest	<a href="#">Link</a>
2024-08-08	[comoferta.com]	darkvault	<a href="#">Link</a>
2024-08-08	[NIDEC CORPORATION]	everest	<a href="#">Link</a>
2024-08-08	[mercadomineiro.com.br]	darkvault	<a href="#">Link</a>
2024-08-07	[hudsoncivil.com.au]	ransomhub	<a href="#">Link</a>
2024-08-07	[www.jgsummit.com.ph]	ransomhub	<a href="#">Link</a>
2024-08-07	[Bayhealth Hospital]	rhysida	<a href="#">Link</a>
2024-08-07	[amplicon.com]	ransomhub	<a href="#">Link</a>
2024-08-06	[infotexim.pe]	ransomhub	<a href="#">Link</a>
2024-08-07	[suandco.com]	madliberator	<a href="#">Link</a>
2024-08-07	[Anderson Oil & Gas]	hunters	<a href="#">Link</a>
2024-08-07	[bonatra.com]	killsec	<a href="#">Link</a>
2024-08-07	[FatBoy Cellular]	meow	<a href="#">Link</a>
2024-08-07	[KLA]	meow	<a href="#">Link</a>
2024-08-07	[HUD User]	meow	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-06	[msprocuradores.es]	madliberator	<a href="#">Link</a>
2024-08-06	[www.carri.com]	alphalocker	<a href="#">Link</a>
2024-08-06	[www.consortioinnova.it]	alphalocker	<a href="#">Link</a>
2024-08-06	[goftac.com/ firsttx.com First Texas Alliance Corp (FTAC)]	alphalocker	<a href="#">Link</a>
2024-08-06	[biw-burger.de]	alphalocker	<a href="#">Link</a>
2024-08-06	[www.sobha.com]	ransomhub	<a href="#">Link</a>
2024-08-06	[Alternate Energy]	play	<a href="#">Link</a>
2024-08-06	[True Blue Environmental]	play	<a href="#">Link</a>
2024-08-06	[Granit Design]	play	<a href="#">Link</a>
2024-08-06	[KinetX]	play	<a href="#">Link</a>
2024-08-06	[Omni Family Health]	hunters	<a href="#">Link</a>
2024-08-06	[IOI Corporation Berhad]	fog	<a href="#">Link</a>
2024-08-06	[Ziba Design]	fog	<a href="#">Link</a>
2024-08-06	[Casco Antiguo]	hunters	<a href="#">Link</a>
2024-08-06	[Fractalia Group]	hunters	<a href="#">Link</a>
2024-08-06	[Banx Systems]	meow	<a href="#">Link</a>
2024-08-05	[Silipos]	cicada3301	<a href="#">Link</a>
2024-08-04	[kierlcpa.com]	lockbit3	<a href="#">Link</a>
2024-08-05	[Square One Coating Systems]	cicada3301	<a href="#">Link</a>
2024-08-05	[Hi-P International]	fog	<a href="#">Link</a>
2024-08-05	[Zon Beachside zonbeachside.com]	dispossessor	<a href="#">Link</a>
2024-08-05	[HP Distribution]	incransom	<a href="#">Link</a>
2024-08-05	[exco-solutions.com]	cactus	<a href="#">Link</a>
2024-08-05	[Maryville Academy]	rhysida	<a href="#">Link</a>
2024-08-04	[notariusze.waw.pl]	killsec	<a href="#">Link</a>
2024-08-04	[Ranney School]	rhysida	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-03	[nursing.com]	ransomexx	<a href="#">Link</a>
2024-08-03	[Bettis Asphalt]	blacksuit	<a href="#">Link</a>
2024-08-03	[fcl.crs]	lockbit3	<a href="#">Link</a>
2024-08-03	[CPA Tax Solutions]	meow	<a href="#">Link</a>
2024-08-03	[LRN]	hunters	<a href="#">Link</a>
2024-08-03	[aikenhousing.org]	blacksuit	<a href="#">Link</a>
2024-08-02	[David E Shambach Architect]	dragonforce	<a href="#">Link</a>
2024-08-02	[Hayes Beer Distributing]	dragonforce	<a href="#">Link</a>
2024-08-02	[Jangho Group]	hunters	<a href="#">Link</a>
2024-08-02	[Khandelwal Laboratories Pvt]	hunters	<a href="#">Link</a>
2024-08-02	[retaildatallc.com]	ransomhub	<a href="#">Link</a>
2024-08-02	[WPG Holdings]	meow	<a href="#">Link</a>
2024-08-02	[National Beverage]	meow	<a href="#">Link</a>
2024-08-02	[PeoplesHR]	meow	<a href="#">Link</a>
2024-08-02	[Dometic Group]	meow	<a href="#">Link</a>
2024-08-02	[Remitano]	meow	<a href="#">Link</a>
2024-08-02	[Premier Equities]	meow	<a href="#">Link</a>
2024-08-01	[Kemlon Products & Development Co Inc]	spacebears	<a href="#">Link</a>
2024-08-02	[q-cells.de]	abyss	<a href="#">Link</a>
2024-08-02	[coinbv.nl]	madliberator	<a href="#">Link</a>
2024-08-01	[Valley Bulk]	cicada3301	<a href="#">Link</a>
2024-08-01	[ENEA Italy]	hunters	<a href="#">Link</a>
2024-08-01	[mcdowallaffleck.com.au]	ransomhub	<a href="#">Link</a>
2024-08-01	[effinghamschools.com]	ransomhub	<a href="#">Link</a>
2024-08-01	[warrendale-wagyu.co.uk]	darkvault	<a href="#">Link</a>
2024-08-01	[Adorna & Guzman Dentistry]	monti	<a href="#">Link</a>
2024-08-01	[Camp Susque]	medusa	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-01	[Ali Gohar]	medusa	Link
2024-08-01	[acsi.org]	blacksuit	<a href="#">Link</a>
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	<a href="#">Link</a>

## 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](https://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](mailto:info@cyberwald.com)

Cyberwald ist ein privates, nicht-kommerzielles Projekt zur Förderung des Bewusstseins für Cybersicherheit.