Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240809

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

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 Rechteausweitung

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

—

Kritische Sicherheitslücke bedroht Unternehmenssoftware Apache OFBiz

Angreifer können Systeme mit Apache OFBiz attackieren und eigenen Code ausführen. Eine dagegen abgesicherte Version steht zum Download bereit.
- Link

—

Unbefugte Zugriffe auf IT-Managementlösung Aruba ClearPass möglich

Die Entwickler von HPE Aruba Networking haben in ClearPass Policy Manager unter anderem eine kritische Sicherheitslücke geschlossen.
- 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	0.988660000	Link
CVE-2023-6895	0.922010000	0.990020000	Link
CVE-2023-6553	0.925190000	0.990400000	Link
CVE-2023-5360	0.903980000	0.988720000	Link
CVE-2023-52251	0.940460000	0.992010000	Link
CVE-2023-4966	0.971280000	0.998270000	Link
CVE-2023-49103	0.962110000	0.995550000	Link
CVE-2023-48795	0.964660000	0.996160000	Link
CVE-2023-47246	0.957550000	0.994730000	Link
CVE-2023-46805	0.937250000	0.991650000	Link
CVE-2023-46747	0.972730000	0.998800000	Link
CVE-2023-46604	0.961790000	0.995480000	Link
CVE-2023-4542	0.928310000	0.990700000	Link
CVE-2023-43208	0.965360000	0.996420000	Link
CVE-2023-43177	0.964550000	0.996140000	Link
CVE-2023-42793	0.969020000	0.997440000	Link
CVE-2023-41265	0.911110000	0.989210000	Link
CVE-2023-39143	0.941900000	0.992190000	Link
CVE-2023-38646	0.906610000	0.988890000	Link
CVE-2023-38205	0.947910000	0.993080000	Link
CVE-2023-38203	0.966410000	0.996670000	Link
CVE-2023-38035	0.974680000	0.999710000	Link
CVE-2023-36845	0.964250000	0.996070000	Link
CVE-2023-3519	0.965340000	0.996400000	Link
CVE-2023-35082	0.968030000	0.997170000	Link
CVE-2023-35078	0.970390000	0.997900000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34993	0.972640000	0.998770000	Link
CVE-2023-34960	0.928290000	0.990690000	Link
CVE-2023-34634	0.925130000	0.990400000	Link
CVE-2023-34468	0.906650000	0.988900000	Link
CVE-2023-34362	0.969450000	0.997590000	Link
CVE-2023-34039	0.944910000	0.992650000	Link
CVE-2023-3368	0.935570000	0.991440000	Link
CVE-2023-33246	0.972140000	0.998570000	Link
CVE-2023-32315	0.970550000	0.997960000	Link
CVE-2023-30625	0.948260000	0.993150000	Link
CVE-2023-30013	0.962790000	0.995710000	Link
CVE-2023-29300	0.968930000	0.997410000	Link
CVE-2023-29298	0.943640000	0.992440000	Link
CVE-2023-28432	0.906190000	0.988850000	Link
CVE-2023-28343	0.923780000	0.990230000	Link
CVE-2023-28121	0.909500000	0.989080000	Link
CVE-2023-27524	0.970600000	0.997980000	Link
CVE-2023-27372	0.973190000	0.999010000	Link
CVE-2023-27350	0.969720000	0.997700000	Link
CVE-2023-26469	0.956500000	0.994570000	Link
CVE-2023-26360	0.965230000	0.996350000	Link
CVE-2023-26035	0.965820000	0.996520000	Link
CVE-2023-25717	0.954250000	0.994160000	Link
CVE-2023-25194	0.968820000	0.997400000	Link
CVE-2023-2479	0.963740000	0.995940000	Link
CVE-2023-24489	0.973540000	0.999150000	Link
CVE-2023-23752	0.956380000	0.994560000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23333	0.958950000	0.994940000	Link
CVE-2023-22527	0.968290000	0.997230000	Link
CVE-2023-22518	0.964890000	0.996200000	Link
CVE-2023-22515	0.973730000	0.999240000	Link
CVE-2023-21839	0.957210000	0.994670000	Link
CVE-2023-21554	0.952830000	0.993860000	Link
CVE-2023-20887	0.970670000	0.998000000	Link
CVE-2023-1671	0.962480000	0.995620000	Link
CVE-2023-0669	0.969440000	0.997580000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Thu, 08 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, 08 Aug 2024

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

Ein entfernter anonymer 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

—

Thu, 08 Aug 2024

[NEU] [hoch] FreeBSD Project FreeBSD OS: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in FreeBSD Project FreeBSD OS ausnutzen, um Sicherheitsvorkehrungen zu umgehen, vertrauliche Informationen preiszugeben, Dateien zu verändern und beliebigen Code als root auszuführen.

- Link

—

Thu, 08 Aug 2024

[NEU] [hoch] Drupal: Mehrere Schwachstellen ermöglichen Codeausführung und Cross Site Scripting

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Drupal ausnutzen, um beliebigen Programmcode auszuführen und einen Cross-Site-Scripting-Angriff durchzuführen.

- Link

—

Thu, 08 Aug 2024

[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Thu, 08 Aug 2024

[UPDATE] [hoch] docker: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Docker ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder Dateien zu manipulieren.

- Link

—

Thu, 08 Aug 2024

[UPDATE] [hoch] Red Hat Ansible Automation Platform: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat Ansible Automation Platform ausnutzen,

um einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren, Phishing-Angriffe durchzuführen oder Cross-Site Scripting (XSS)-Angriffe auszuführen. Einige dieser Schwachstellen erfordern eine Benutzerinteraktion, um sie erfolgreich auszunutzen.

- Link

—

Thu, 08 Aug 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in verschiedenen Komponenten von Red Hat Enterprise Linux ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand auszulösen.

- Link

—

Thu, 08 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, 08 Aug 2024

[UPDATE] [hoch] Red Hat Ansible Automation Platform: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat Ansible Automation Platform ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand erzeugen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder Cross-Site-Scripting (XSS)-Angriffe durchzuführen.

- Link

—

Thu, 08 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, 08 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, 08 Aug 2024

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

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

- Link

—

Thu, 08 Aug 2024

[UPDATE] [hoch] docker: Schwachstelle ermöglicht Privilegieneskalation

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

- Link

—

Thu, 08 Aug 2024

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

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

- Link

—

Thu, 08 Aug 2024

[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen

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

- Link

—

Wed, 07 Aug 2024

[UPDATE] [hoch] PostgreSQL: Mehrere Schwachstellen

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um Informationen offenzulegen, beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Wed, 07 Aug 2024

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

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

- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/8/2024	[Debian dsa-5744 : thunderbird - security update]	critical
8/8/2024	[Ubuntu 16.04 LTS / 18.04 LTS : Salt vulnerabilities (USN-6948-1)]	critical
8/8/2024	[EulerOS 2.0 SP11 : git (EulerOS-SA-2024-2098)]	critical
8/8/2024	[EulerOS 2.0 SP11 : git (EulerOS-SA-2024-2081)]	critical
8/8/2024	[Cisco Smart Software Manager On-Prem Password Change Vulnerability (CVE-2024-20419)]	critical
8/8/2024	[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6951-1)]	high
8/8/2024	[Ubuntu 22.04 LTS / 24.04 LTS : Linux kernel vulnerabilities (USN-6949-1)]	high
8/8/2024	[EulerOS 2.0 SP11 : libarchive (EulerOS-SA-2024-2085)]	high
8/8/2024	[EulerOS 2.0 SP11 : libxml2 (EulerOS-SA-2024-2088)]	high
8/8/2024	[EulerOS 2.0 SP11 : glibc (EulerOS-SA-2024-2099)]	high
8/8/2024	[EulerOS 2.0 SP11 : libarchive (EulerOS-SA-2024-2102)]	high
8/8/2024	[EulerOS 2.0 SP11 : python-pip (EulerOS-SA-2024-2110)]	high
8/8/2024	[EulerOS 2.0 SP11 : python-pip (EulerOS-SA-2024-2093)]	high
8/8/2024	[EulerOS 2.0 SP11 : openssl (EulerOS-SA-2024-2090)]	high
8/8/2024	[EulerOS 2.0 SP11 : openssh (EulerOS-SA-2024-2106)]	high
8/8/2024	[EulerOS 2.0 SP11 : libxml2 (EulerOS-SA-2024-2105)]	high
8/8/2024	[EulerOS 2.0 SP11 : openssh (EulerOS-SA-2024-2089)]	high
8/8/2024	[EulerOS 2.0 SP11 : systemd (EulerOS-SA-2024-2095)]	high

Datum	Schwachstelle	Bewertung
8/8/2024	[EulerOS 2.0 SP11 : python-idna (EulerOS-SA-2024-2091)]	high
8/8/2024	[EulerOS 2.0 SP11 : less (EulerOS-SA-2024-2101)]	high
8/8/2024	[EulerOS 2.0 SP11 : glibc (EulerOS-SA-2024-2082)]	high
8/8/2024	[EulerOS 2.0 SP11 : openssl (EulerOS-SA-2024-2107)]	high
8/8/2024	[EulerOS 2.0 SP11 : python-idna (EulerOS-SA-2024-2108)]	high
8/8/2024	[EulerOS 2.0 SP11 : less (EulerOS-SA-2024-2084)]	high
8/8/2024	[EulerOS 2.0 SP11 : systemd (EulerOS-SA-2024-2112)]	high
8/8/2024	[EulerOS 2.0 SP11 : libndp (EulerOS-SA-2024-2086)]	high
8/8/2024	[EulerOS 2.0 SP11 : libndp (EulerOS-SA-2024-2103)]	high
8/8/2024	[Siemens RUGGEDCOM Exposure of Sensitive Information to an Unauthorized Actor (CVE-2023-52237)]	high
8/8/2024	[Siemens RUGGEDCOM Exposure of Sensitive System Information to an Unauthorized Control Sphere (CVE-2024-39675)]	high
8/8/2024	[Yokogawa CENTUM Controller Improper Access Control (CVE-2024-5650)]	high
8/8/2024	[Emerson Ovation OCR400 Controller Stack-Based Buffer Overflow (CVE-2019-10967)]	high
8/8/2024	[Emerson Ovation OCR400 Controller Heap-Based Buffer Overflow (CVE-2019-10965)]	high
8/8/2024	[Rockwell Logix Controllers Unprotected Alternate Channel (CVE-2024-6242)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Thu, 08 Aug 2024

Calibre 7.15.0 Python Code Injection

This Metasploit module exploits a Python code injection vulnerability in the Content Server compo-

nent 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

—

” “Thu, 08 Aug 2024

Apple libresolve Heap Buffer Overflow

libresolv’s DNS packet handler suffered from heap out-of-bounds write to infinite-loop denial of service vulnerabilities. This is a proof of concept exploit from Google.

- Link

—

” “Thu, 08 Aug 2024

Apache log4j2 Code Execution

Log4j 2.15.0 was released to address the widely reported JNDI Remote Code Execution (RCE) (CVE-

2021-44228) vulnerability in Log4j. Shortly thereafter, 2.16.0 was released to address a Denial of Service (DoS) vulnerability (CVE-2021-45046). When examining the 2.15.0 release, Google security engineers found several issues with the Log4j 2.15.0 patch that showed that the severity of the issue addressed in 2.16 was in fact worse than initially understood. This is Google's proof of concept exploit.
- Link

—

" "Thu, 08 Aug 2024

Surface Pro 3 BIOS False Health Attestation / TPM Carte Blanche

On Surface Pro 3 with the SHA1 and SHA256 PCRs enabled on the TPM, BIOS version 3.11.2550 and earlier, only the SHA1 PCRs are extended by the firmware. This means that an adversary can boot into an unmeasured OS and extend the PCRs with false measurements to obtain false attestations. This is a proof of concept exploit from Google.
- Link

—

" "Thu, 08 Aug 2024

Linux xt_compat_target_from_user Heap Out-Of-Bounds Write

A heap out-of-bounds write affecting Linux since v2.6.19-rc1 was discovered in net/netfilter/x_tables.c. This is the proof of concept exploit produced by Google.
- Link

—

" "Thu, 08 Aug 2024

Linux KVM VM_IO|VM_PFNMAP VMA Mishandling

Improper handling of VM_IO|VM_PFNMAP vmas in KVM can bypass RO checks and can lead to pages being freed while still accessible by the VMM and guest. This is a proof of concept exploit produced by Google.
- Link

—

" "Thu, 08 Aug 2024

Windows Firewall Control 6.11.0 Unquoted Service Path

Windows Firewall Control version 6.11.0 suffers from an unquoted service path vulnerability.
- Link

—

" "Thu, 08 Aug 2024

Employee Management System 1.0 SQL Injection

Employee Management System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass. Original discovery of this finding is attributed to Ozlem Balci in January of 2024.
- Link

—

” “Thu, 08 Aug 2024

E-Commerce Site Using PHP PDO 1.0 Insecure Settings

E-Commerce Site using PHP PDO version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Thu, 08 Aug 2024

Bhojon Restaurant Management System 2.8 Insecure Settings

Bhojon Restaurant Management System version 2.8 suffers from an ignored default credential vulnerability.

- Link

—

” “Wed, 07 Aug 2024

Mailcow TFA Authentication Bypass

This is a proof of concept exploit to bypass two factor authentication in Mailcow versions prior to 2024-07.

- 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

—

” “Tue, 06 Aug 2024

ZDI-24-1101: Apple macOS Metal Framework KTX Image Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1100: SMARTBEAR SoapUI unpackageAll Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1099: Apache OFBiz resolveURI Authentication Bypass Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1098: (0Day) Microsoft Windows Error Reporting Service Missing Authorization Arbitrary Process Termination Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1097: (0Day) Microsoft GitHub Dev-Containers Improper Privilege Management Privilege Escalation Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1096: (0Day) Microsoft Office Visio EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1095: (0Day) Microsoft Office Visio DXF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1094: (0Day) Microsoft Office Visio EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1093: (0Day) Microsoft Office Visio EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1092: (0Day) Microsoft Office Visio DXF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1091: (0Day) Microsoft Windows DirectComposition Out-Of-Bounds Read Denial-of-Service Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1090: (0Day) Microsoft Windows DirectComposition Null Pointer Dereference Denial-of-Service Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1089: (0Day) Microsoft Office Visio DXF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 06 Aug 2024

ZDI-24-1088: (0Day) Microsoft 3D Viewer GLB File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1087: (0Day) oFono SMS Decoder Stack-based Buffer Overflow Privilege Escalation Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1086: (0Day) oFono SimToolKit Heap-based Buffer Overflow Privilege Escalation Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1085: (0Day) oFono SimToolKit Heap-based Buffer Overflow Privilege Escalation Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1084: (0Day) oFono SimToolKit Heap-based Buffer Overflow Privilege Escalation Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1083: (0Day) oFono SimToolKit Heap-based Buffer Overflow Privilege Escalation Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1082: (0Day) (Pwn2Own) oFono AT CMGR Command Uninitialized Variable Information Disclosure Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1081: (0Day) (Pwn2Own) oFono AT CMT Command Uninitialized Variable Information

Disclosure Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1080: (0Day) (Pwn2Own) oFono AT CMGL Command Uninitialized Variable Information Disclosure Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1079: (0Day) (Pwn2Own) oFono CUSD Stack-based Buffer Overflow Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1078: (0Day) (Pwn2Own) oFono CUSD AT Command Stack-based Buffer Overflow Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1077: (0Day) (Pwn2Own) oFono QMI SMS Handling Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1076: Microsoft Windows Menu DC Color Space Use-After-Free Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1075: Microsoft PowerShell Reference for Office Products officedocs-cdn Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1074: Microsoft PowerShell Gallery psg-prod-centralus Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1073: Microsoft Azure uAMQP azure-iot-sdks-ci Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1072: Microsoft CameraTraps cameratracrsppftkje Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1071: Microsoft Azure GPT ALE palantirdemoacr Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1070: Microsoft Partner Resources openhacks Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1069: Microsoft Technical Case Studies athena-dashboard Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1068: Microsoft Azure ML.NET Samples mlnetfilestorage Uncontrolled Search Path Element Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1067: Microsoft Azure CollectSFData docs-analytics-eus Uncontrolled Search Path Element Impersonation Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1066: Microsoft Azure DataStoriesSamples machinelearningdatasets Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1065: Microsoft Azure Availability Monitor for Kafka esnewdeveastdockerregistry Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1064: Microsoft AirSim airsimci Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1063: Microsoft Reactor Workshops reactorworkshops Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1062: Microsoft Fluid Framework prague Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1061: Microsoft What The Hack docsmsftpdfs Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1060: Microsoft Azure Aztack aztack1528763526 Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1059: Microsoft Azure Linux Automation konkaciwestus1 Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1058: Microsoft Azure NodeJS LogPoint logpointsassets Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1057: Trimble SketchUp Pro SKP File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1056: Trimble SketchUp SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1055: Trimble SketchUp SKP File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Aug 2024

ZDI-24-1054: Trimble SketchUp Viewer SKP File Parsing Heap-based Buffer Overflow Remote Code Execution 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
2024-08-06	Nilörn	[SWE]	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
2024-08-09	[Gramercy Surgery Center Data Leak]	everest	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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.