Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240813

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

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

—

VPN-Clients und Passwortmanager betroffen: Klartextpasswort im Prozessspeicher

Wegen einer Lücke unter anderem in VPN-Clients und Passwortmanagern bleiben vertrauliche Daten auch nach Abmeldung im Prozess-Speicher und sind auslesbar.

- Link

—

CPU-Sicherheitslücke in AMD-Prozessoren ermöglicht Malware-Infektionen

Sicherheitsforscher haben eine als Sinkclose bezeichnete Sicherheitslücke in AMD-CPUs 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 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

—

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	0.988680000	Link
CVE-2023-6895	0.922010000	0.990040000	Link
CVE-2023-6553	0.925190000	0.990440000	Link
CVE-2023-5360	0.903980000	0.988740000	Link
CVE-2023-52251	0.944080000	0.992520000	Link
CVE-2023-4966	0.971280000	0.998300000	Link
CVE-2023-49103	0.962110000	0.995580000	Link
CVE-2023-48795	0.964660000	0.996170000	Link
CVE-2023-47246	0.953860000	0.994130000	Link
CVE-2023-46805	0.937250000	0.991690000	Link
CVE-2023-46747	0.972820000	0.998890000	Link
CVE-2023-46604	0.961790000	0.995510000	Link
CVE-2023-4542	0.928310000	0.990750000	Link
CVE-2023-43208	0.966400000	0.996670000	Link
CVE-2023-43177	0.964550000	0.996150000	Link
CVE-2023-42793	0.969020000	0.997450000	Link
CVE-2023-41265	0.911110000	0.989250000	Link
CVE-2023-39143	0.939130000	0.991920000	Link
CVE-2023-38646	0.906610000	0.988930000	Link
CVE-2023-38205	0.947910000	0.993100000	Link
CVE-2023-38203	0.966410000	0.996690000	Link
CVE-2023-38146	0.920720000	0.989880000	Link
CVE-2023-38035	0.974680000	0.999710000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.966270000	0.996650000	Link
CVE-2023-3519	0.965340000	0.996420000	Link
CVE-2023-35082	0.966130000	0.996610000	Link
CVE-2023-35078	0.970390000	0.997930000	Link
CVE-2023-34993	0.972640000	0.998810000	Link
CVE-2023-34960	0.928290000	0.990740000	Link
CVE-2023-34634	0.925130000	0.990430000	Link
CVE-2023-34468	0.906650000	0.988930000	Link
CVE-2023-34362	0.971000000	0.998180000	Link
CVE-2023-34039	0.947770000	0.993040000	Link
CVE-2023-3368	0.932420000	0.991220000	Link
CVE-2023-33246	0.972140000	0.998590000	Link
CVE-2023-32315	0.970550000	0.997990000	Link
CVE-2023-30625	0.953800000	0.994120000	Link
CVE-2023-30013	0.962380000	0.995640000	Link
CVE-2023-29300	0.968930000	0.997420000	Link
CVE-2023-29298	0.943640000	0.992490000	Link
CVE-2023-28432	0.906190000	0.988890000	Link
CVE-2023-28343	0.942300000	0.992300000	Link
CVE-2023-28121	0.909500000	0.989110000	Link
CVE-2023-27524	0.970600000	0.998010000	Link
CVE-2023-27372	0.972120000	0.998580000	Link
CVE-2023-27350	0.969720000	0.997720000	Link
CVE-2023-26469	0.956020000	0.994550000	Link
CVE-2023-26360	0.965230000	0.996370000	Link
CVE-2023-26035	0.967360000	0.996950000	Link
CVE-2023-25717	0.954250000	0.994220000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-25194	0.968820000	0.997400000	Link
CVE-2023-2479	0.963740000	0.995950000	Link
CVE-2023-24489	0.973870000	0.999310000	Link
CVE-2023-23752	0.956380000	0.994600000	Link
CVE-2023-23333	0.958950000	0.994970000	Link
CVE-2023-22527	0.968290000	0.997240000	Link
CVE-2023-22518	0.964890000	0.996210000	Link
CVE-2023-22515	0.973250000	0.999060000	Link
CVE-2023-21839	0.955020000	0.994360000	Link
CVE-2023-21554	0.952830000	0.993930000	Link
CVE-2023-20887	0.970670000	0.998030000	Link
CVE-2023-1671	0.962480000	0.995640000	Link
CVE-2023-0669	0.969440000	0.997610000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 12 Aug 2024

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

Ein Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, seine Privilegien zu erweitern, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.

- Link

—

Mon, 12 Aug 2024

[UPDATE] [hoch] GNU libc: Schwachstelle ermöglicht Codeausführung

Ein Angreifer kann eine Schwachstelle in GNU libc ausnutzen, um einen Denial-of-Service-Zustand zu verursachen, Code auszuführen oder seine Privilegien zu erweitern.

- Link

—

Mon, 12 Aug 2024

[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Oracle MySQL ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- Link

—

Mon, 12 Aug 2024

[NEU] [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

—

Mon, 12 Aug 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Mon, 12 Aug 2024

[UPDATE] [hoch] rsyslog: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in rsyslog ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Mon, 12 Aug 2024

[UPDATE] [hoch] Ruby on Rails: Schwachstelle ermöglicht Codeausführung

Ein entfernter Angreifer kann eine Schwachstelle in Ruby on Rails ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 12 Aug 2024

[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle MySQL ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- Link

—

Mon, 12 Aug 2024

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um einen Denial of Service Angriff durchzuführen, um Sicherheitsmechanismen zu umgehen und um unbekannte Auswirkungen zu erzielen.

- Link

—

Mon, 12 Aug 2024

[UPDATE] [hoch] strongSwan: Schwachstelle ermöglicht Codeausführung und DoS

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in strongSwan ausnutzen, um einen Denial of Service zu verursachen und beliebigen Programmcode auszuführen.

- Link

—

Mon, 12 Aug 2024

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

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

- Link

—

Mon, 12 Aug 2024

[UPDATE] [hoch] strongSwan: Schwachstelle ermöglicht Codeausführung und DoS

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in strongSwan ausnutzen, um beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Mon, 12 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

—

Mon, 12 Aug 2024

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmaßnahmen zu umgehen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Mon, 12 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

—

Mon, 12 Aug 2024

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

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

- Link

—

Mon, 12 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

—

Mon, 12 Aug 2024

[UPDATE] [kritisch] Cisco Smart Software Manager On-Prem: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Cisco Smart Software Manager On-Prem ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

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

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/12/2024	[Apache OFBiz < 18.12.15 Remote Code Execution]	critical
8/12/2024	[Apache OFBiz < 18.12.13 Path Traversal]	critical
8/12/2024	[Fedora 40 : neatvnc (2024-1fbf7f22e0)]	critical
8/12/2024	[Fedora 39 : neatvnc (2024-7250fa4a78)]	critical
8/12/2024	[Fedora 39 : firefox / nss (2024-4fcf85b0ff)]	critical
8/12/2024	[Fedora 40 : firefox / nss (2024-7f0a88301b)]	critical
8/12/2024	[Debian dsa-5747 : affs-modules-5.10.0-29-4kc-malta-di - security update]	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
8/12/2024	[Apache OFBiz < 18.12.11 Server-Side Request Forgery]	high
8/12/2024	[Fedora 39 : chromium (2024-b60f51180f)]	high
8/12/2024	[Apache RocketMQ < 5.3.0 Information Disclosure (CVE-2024-23321)]	high
8/12/2024	[AlmaLinux 8 : httpd:2.4 (ALSA-2024:5193)]	high
8/12/2024	[Ubuntu 24.04 LTS : Linux kernel (OEM) vulnerabilities (USN-6955-1)]	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

Datum	Schwachstelle	Bewertung
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

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Mon, 12 Aug 2024

Computer Laboratory Management 1.0 SQL Injection

Computer Laboratory Management version 1.0 suffers from a remote authenticated SQL injection vulnerability.

- Link

—

” “Mon, 12 Aug 2024

Courier Management System 2020-1.0 SQL Injection

Courier Management System version 2020-1.0 suffers from multiple remote SQL injection vulnerabilities.

- Link

—

” “Mon, 12 Aug 2024

Backdoor.Win32.Nightmare.25 MVID-2024-0687 Code Execution

Backdoor.Win32.Nightmare.25 malware suffers from a code execution vulnerability.

- Link

—

” “Mon, 12 Aug 2024

Gas Agency Management 2022 Cross Site Request Forgery

Gas Agency Management version 2022 suffers from a cross site request forgery vulnerability.

- Link

—

” “Mon, 12 Aug 2024

Garden Gate 2.6 SQL Injection

Garden Gate version 2.6 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 12 Aug 2024

Goati Track 1.0-2023 Insecure Settings

Gaati Track version 1.0-2023 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 12 Aug 2024

Farmacia Gama 1.0 Insecure Direct Object Reference

Farmacia Gama version 1.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Mon, 12 Aug 2024

Employee Management System 1.0 Insecure Settings

Employee Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 12 Aug 2024

Computer And Mobile Repair Shop Management System 1.0 Cross Site Request Forgery

Computer and Mobile Repair Shop Management System version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “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 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

—

”

4.2 0-Days der letzten 5 Tage

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
2024-08-11	Université Paris-Saclay	[FRA]	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
2024-08-07	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
2024-08-12	[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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-08-05	[Silipos]	cicada3301	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-08-01	[Kemlon Products & Development Co Inc]	spacebears	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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.