Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240724

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

Software-Distributionssystem TeamCity erinnert sich an gelöschte Zugangstoken

Angreifer können an sechs mittlerweile geschlossenen Sicherheitslücken in JetBrain TeamCity ansetzen.

- Link

—

Backup-System Data Protection Advisor von Dell vielfältig angreifbar

Dell hat mehrere Sicherheitslücken in Data Protection Advisor geschlossen. Es kann Schadcode auf Systeme gelangen.

- Link

—

BIOS-Sicherheitslücke gefährdet unzählige HP-PCs

Angreifer können viele Desktopcomputer von HP mit Schadcode attackieren.

- Link

—

Sicherheitsupdates: Angreifer können Sonicwall-Firewalls lahmlegen

Einige Firewalls von Sonicwall sind verwundbar. Attacken könnten bevorstehen.

- Link

—

SolarWinds Access Rights Manager: Angreifer mit Systemrechten und Schadcode

Die Entwickler haben in SolarWinds ARM acht kritische Sicherheitslücken geschlossen.

- Link

—

Schlupfloch für Schadcode in Ivanti Endpoint Manager geschlossen

Stimmen die Voraussetzungen, sind Attacken auf Ivanti Endpoint Manager möglich. Ein Sicherheitspatch schafft Abhilfe.

- Link

—

Atlassian Bamboo: Angreifer können Entwicklungsumgebungen kompromittieren

Es sind Attacken auf Atlassian Bamboo Data Center und Server vorstellbar. Dagegen abgesicherte Version sind erschienen.

- Link

—

Sicherheitslücke mit Höchstwertung in Cisco Smart Software Manager On-Prem

Cisco schließt unter anderem eine Passwort- und Root-Sicherheitslücke in SSM On-Prem und Secure

Email Gateway.
- Link

—

Critical Patch Update: Oracles Quartalsupdate liefert 386 Sicherheitspatches

Angreifer können kritische Lücken in unter anderem Oracle HTTP Server oder MySQL Cluster ausnutzen.
- Link

—

Root-Schwachstelle bedroht KI-Gadget Rabbit R1

Angreifer können das KI-Gadget Rabbit R1 kompromittieren. Bislang gibt es keinen Sicherheitspatch.
- 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	0.965050000	0.996200000	Link
CVE-2023-6895	0.922010000	0.989930000	Link
CVE-2023-6553	0.937510000	0.991550000	Link
CVE-2023-5360	0.903980000	0.988600000	Link
CVE-2023-52251	0.938200000	0.991640000	Link
CVE-2023-4966	0.971290000	0.998180000	Link
CVE-2023-49103	0.953130000	0.993860000	Link
CVE-2023-48795	0.965740000	0.996430000	Link
CVE-2023-47246	0.948140000	0.993020000	Link
CVE-2023-46805	0.958670000	0.994810000	Link
CVE-2023-46747	0.972730000	0.998710000	Link
CVE-2023-46604	0.963510000	0.995810000	Link
CVE-2023-4542	0.921170000	0.989820000	Link
CVE-2023-43208	0.964870000	0.996130000	Link
CVE-2023-43177	0.962660000	0.995600000	Link
CVE-2023-42793	0.970960000	0.998040000	Link
CVE-2023-41265	0.905890000	0.988720000	Link
CVE-2023-39143	0.938190000	0.991630000	Link
CVE-2023-38646	0.910550000	0.989020000	Link
CVE-2023-38205	0.954590000	0.994140000	Link
CVE-2023-38203	0.966000000	0.996470000	Link
CVE-2023-38146	0.915710000	0.989380000	Link
CVE-2023-38035	0.974400000	0.999550000	Link
CVE-2023-36845	0.961840000	0.995430000	Link
CVE-2023-3519	0.965360000	0.996320000	Link
CVE-2023-35082	0.968030000	0.997090000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-35078	0.968330000	0.997180000	Link
CVE-2023-34993	0.972880000	0.998790000	Link
CVE-2023-34960	0.929370000	0.990730000	Link
CVE-2023-34634	0.927960000	0.990540000	Link
CVE-2023-34468	0.906650000	0.988790000	Link
CVE-2023-34362	0.969450000	0.997490000	Link
CVE-2023-34039	0.940490000	0.991900000	Link
CVE-2023-3368	0.933870000	0.991190000	Link
CVE-2023-33246	0.972610000	0.998660000	Link
CVE-2023-32315	0.973620000	0.999120000	Link
CVE-2023-30625	0.948260000	0.993050000	Link
CVE-2023-30013	0.962250000	0.995500000	Link
CVE-2023-29300	0.968930000	0.997330000	Link
CVE-2023-29298	0.943640000	0.992340000	Link
CVE-2023-28771	0.902140000	0.988480000	Link
CVE-2023-28343	0.949510000	0.993230000	Link
CVE-2023-28121	0.909760000	0.988960000	Link
CVE-2023-27524	0.970300000	0.997800000	Link
CVE-2023-27372	0.972890000	0.998790000	Link
CVE-2023-27350	0.970130000	0.997720000	Link
CVE-2023-26469	0.951490000	0.993540000	Link
CVE-2023-26360	0.962310000	0.995540000	Link
CVE-2023-26035	0.967100000	0.996800000	Link
CVE-2023-25717	0.956860000	0.994520000	Link
CVE-2023-25194	0.968820000	0.997310000	Link
CVE-2023-2479	0.963740000	0.995880000	Link
CVE-2023-24489	0.973720000	0.999160000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23752	0.954250000	0.994070000	Link
CVE-2023-23397	0.901800000	0.988450000	Link
CVE-2023-23333	0.959750000	0.995020000	Link
CVE-2023-22527	0.970550000	0.997870000	Link
CVE-2023-22518	0.964890000	0.996130000	Link
CVE-2023-22515	0.973590000	0.999120000	Link
CVE-2023-21839	0.957210000	0.994570000	Link
CVE-2023-21554	0.952830000	0.993780000	Link
CVE-2023-20887	0.970170000	0.997740000	Link
CVE-2023-1671	0.962480000	0.995560000	Link
CVE-2023-0669	0.969440000	0.997480000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 23 Jul 2024

[UPDATE] [UNGEPATCHT] [kritisch] Linksys WRT54G Router: Schwachstelle ermöglicht Codeausführung und DoS

Ein entfernter, anonymer Angreifer kann eine Schwachstelle im Linksys WRT54G Router ausnutzen, um beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Tue, 23 Jul 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

—

Tue, 23 Jul 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

—

Tue, 23 Jul 2024

[UPDATE] [hoch] RADIUS: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein lokaler Angreifer kann eine Schwachstelle im RADIUS Protokoll ausnutzen, um Sicherheitsvorkehrungen zu umgehen.
- Link

—

Tue, 23 Jul 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Firefox ESR ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmechanismen zu umgehen, Daten zu manipulieren und den Benutzer zu täuschen.
- Link

—

Tue, 23 Jul 2024

[NEU] [hoch] Dell Data Protection Advisor: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Dell Data Protection Advisor ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Tue, 23 Jul 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

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

—

Tue, 23 Jul 2024

[UPDATE] [hoch] Intel PROSet Wireless WiFi Software: Mehrere Schwachstellen ermöglichen Denial of Service

Ein Angreifer aus einem angrenzenden Netzwerk kann mehrere Schwachstellen in Intel PROSet Wireless WiFi Software ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

Tue, 23 Jul 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

—

Tue, 23 Jul 2024

[UPDATE] [hoch] Ghostscript: Mehrere Schwachstellen

Ein entfernter anonymer oder ein lokaler Angreifer kann mehrere Schwachstellen in Ghostscript ausnutzen, um Informationen offenzulegen oder beliebigen Code auszuführen.
- Link

—

Tue, 23 Jul 2024

[UPDATE] [hoch] Exim: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Exim ausnutzen, um Sicherheitsvorkehrungen zu umgehen.
- Link

—

Tue, 23 Jul 2024

[UPDATE] [hoch] Node.js: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Code auszuführen oder um Sicherheitsmaßnahmen zu umgehen.
- Link

—

Tue, 23 Jul 2024

[UPDATE] [hoch] Django: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Django ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder vertrauliche Informationen offenzulegen.
- Link

—

Tue, 23 Jul 2024

[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen

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

—

Tue, 23 Jul 2024

[NEU] [hoch] PyTorch: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in PyTorch ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder einen unspezifischen Angriff durchzuführen.

- Link

—

Tue, 23 Jul 2024

[NEU] [hoch] Siemens SICAM: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Siemens SICAM ausnutzen, um seine Privilegien zu erhöhen oder die Firmware-Version herabzustufen.

- Link

—

Mon, 22 Jul 2024

[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen, um einen Denial of Service Zustand herbeizuführen und um Sicherheitsmechanismen zu umgehen.

- Link

—

Mon, 22 Jul 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

—

Mon, 22 Jul 2024

[UPDATE] [hoch] Oracle Retail Applications: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Oracle Retail Applications ausnutzen, um dadurch die Integrität, Vertraulichkeit und Verfügbarkeit zu gefährden.

- Link

—

Mon, 22 Jul 2024

[UPDATE] [hoch] Jenkins: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Jenkins ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder Cross-Site Scripting (XSS)-Angriffe durchzuführen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
7/23/2024	[Photon OS 5.0: Nodejs PHSA-2023-5.0-0082]	critical
7/23/2024	[Photon OS 4.0: Openssh PHSA-2023-4.0-0444]	critical
7/23/2024	[Photon OS 4.0: Linux PHSA-2023-4.0-0458]	critical
7/23/2024	[Slackware Linux 15.0 mozilla-thunderbird Multiple Vulnerabilities (SSA:2024-205-03)]	critical
7/23/2024	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : Apache ActiveMQ vulnerabilities (USN-6910-1)]	critical
7/23/2024	[Oracle Linux 9 : httpd (ELSA-2024-4726)]	critical
7/23/2024	[Oracle Linux 8 : httpd:2.4 (ELSA-2024-4720)]	critical
7/23/2024	[EulerOS 2.0 SP8 : tigervnc (EulerOS-SA-2024-2062)]	critical
7/23/2024	[EulerOS 2.0 SP8 : xorg-x11-server (EulerOS-SA-2024-2063)]	critical
7/23/2024	[Photon OS 5.0: Linux PHSA-2023-5.0-0130]	high
7/23/2024	[Photon OS 5.0: Linux PHSA-2023-5.0-0170]	high
7/23/2024	[Photon OS 4.0: Apache PHSA-2024-4.0-0574]	high
7/23/2024	[Photon OS 4.0: Nmap PHSA-2023-4.0-0517]	high
7/23/2024	[Slackware Linux 15.0 / current aaa_glibc-solibs Multiple Vulnerabilities (SSA:2024-205-02)]	high
7/23/2024	[Slackware Linux 15.0 / current bind Multiple Vulnerabilities (SSA:2024-205-01)]	high
7/23/2024	[RHEL 8 : krb5 (RHSA-2024:4743)]	high
7/23/2024	[RHEL 9 : libuv (RHSA-2024:4756)]	high
7/23/2024	[RHEL 9 : edk2 (RHSA-2024:4749)]	high
7/23/2024	[RHEL 8 : kernel (RHSA-2024:4731)]	high
7/23/2024	[RHEL 9 : runc (RHSA-2024:4762)]	high
7/23/2024	[RHEL 8 : kernel (RHSA-2024:4740)]	high
7/23/2024	[RHEL 8 : krb5 (RHSA-2024:4734)]	high
7/23/2024	[RHEL 9 : containernetworking-plugins (RHSA-2024:4761)]	high

Datum	Schwachstelle	Bewertung
7/23/2024	[RHEL 9 : libreoffice (RHSA-2024:4755)]	high
7/23/2024	[RHEL 8 : kernel-rt (RHSA-2024:4729)]	high
7/23/2024	[Ubuntu 16.04 LTS / 18.04 LTS : HAProxy vulnerability (USN-6530-2)]	high
7/23/2024	[EulerOS 2.0 SP8 : ImageMagick (EulerOS-SA-2024-2058)]	high
7/23/2024	[Siemens SIMATIC and SCALANCE Products Encryption Strength (CVE-2023-0464)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Tue, 23 Jul 2024

Perten Instruments Process Plus Software 1.11.6507.0 LFI / Hardcoded Credentials

Perten Instruments Process Plus Software versions 1.11.6507.0 and below suffer from local file inclusion, hardcoded credential, and execution with unnecessary privilege vulnerabilities.

- Link

—

” “Tue, 23 Jul 2024

LMS ZAI 6.1 Insecure Settings

LMS ZAI version 6.1 suffers from an ignored default credential vulnerability.

- Link

—

” “Tue, 23 Jul 2024

Quick Job 2.4 Insecure Direct Object Reference

Quick Job version 2.4 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Tue, 23 Jul 2024

PPDB ONLINE 1.3 Administrative Page Disclosure

PPDB ONLINE version 1.3 appears to suffer from an administrative page disclosure issue.

- Link

—

” “Tue, 23 Jul 2024

PHP MaXiMuS 2.5.2 Cross Site Scripting

PHP MaXiMuS version 2.5.2 suffers from a cross site scripting vulnerability.

- Link

—

” “Tue, 23 Jul 2024

NUKE SENTINEL 2.5.2 Cross Site Scripting

NUKE SENTINEL version 2.5.2 suffers from a cross site scripting vulnerability.

- Link

—

” “Tue, 23 Jul 2024

Minfotech CMS 2.0 SQL Injection

Minfotech CMS version 2.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Tue, 23 Jul 2024

eDesign CMS 2.0 Insecure Direct Object Reference

eDesign CMS version 2.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Mon, 22 Jul 2024

Softing Secure Integration Server 1.22 Remote Code Execution

This Metasploit module chains two vulnerabilities to achieve authenticated remote code execution against Softing Secure Integration Server version 1.22. In CVE-2022-1373, the restore configuration feature is vulnerable to a directory traversal vulnerability when processing zip files. When using the ”restore configuration” feature to upload a zip file containing a path traversal file which is a dll called ..\..\..\..\..\..\..\..\..\..\..\Windows\System32\wbem\wbemcomn.dll. This causes the file C:\Windows\System32\wbem\wbemcomn.dll to be created and executed upon touching the disk. In CVE-2022-2334, the planted wbemcomn.dll is used in a DLL hijacking attack when Softing Secure Integration Server restarts upon restoring configuration, which allows us to execute arbitrary code on the target system. The chain demonstrated in Pwn2Own used a signature instead of a password. The signature was acquired by running an ARP spoofing attack against the local network where the Softing SIS server was located. A username is also required for signature authentication. A custom DLL can be provided to use in the exploit instead of using the default MSF-generated one.

- Link

—

” “Mon, 22 Jul 2024

Ghostscript Command Execution / Format String

This Metasploit module exploits a format string vulnerability in Ghostscript versions before 10.03.1 to achieve a SAFER sandbox bypass and execute arbitrary commands. This vulnerability is reachable via libraries such as ImageMagick. This exploit only works against Ghostscript versions 10.03.0 and 10.01.2. Some offsets adjustment will probably be needed to make it work with other versions.

- Link

—

” “Mon, 22 Jul 2024

Collateral Damage CVE-2024-30088 Privilege Escalation

Collateral Damage is a kernel exploit for Xbox SystemOS using CVE-2024-30088. It targets Xbox One and Xbox Series consoles running kernel versions 25398.4478, 25398.4908, and 25398.4909. The initial entrypoint is via the Game Script UWP application.

- Link

—

” “Mon, 22 Jul 2024

Adobe Commerce / Magento Open Source XML Injection / User Impersonation

Adobe Commerce and Magento Open Source are affected by an XML injection vulnerability that could result in arbitrary code execution. An attacker could exploit this vulnerability by sending a crafted XML document that references external entities. Exploitation of this issue does not require user interaction. Versions Affected include Adobe Commerce and Magento Open Source 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8, and earlier. This exploit uses the arbitrary file reading aspect of the issue to impersonate a user.

- Link

—

” “Mon, 22 Jul 2024

Xhibiter NFT Marketplace 1.10.2 Cross Site Scripting

Xhibiter NFT Marketplace version 1.10.2 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 22 Jul 2024

eStore CMS 2.0 SQL Injection

eStore CMS version 2.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 22 Jul 2024

Clenix 1.0 Insecure Direct Object Reference

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

- Link

—

” “Mon, 22 Jul 2024

Candy Redis 2.1.2 Admin Page Disclosure

Candy Redis version 2.1.2 appears to suffer from an administrative page disclosure issue.

- Link

—

” “Mon, 22 Jul 2024

Agop CMS 1.0 Insecure Direct Object Reference

Agop CMS version 1.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Thu, 18 Jul 2024

PowerVR Dangling Page Table Entry

PowerVR has an issue with missing tracking of multiple sparse mappings in DevmemIntChangeSparse2() that leads to a dangling page table entry.

- Link

—

” “Wed, 17 Jul 2024

Xenforo 2.2.15 Remote Code Execution

XenForo versions 2.2.15 and below suffer from a remote code execution vulnerability in the Template system.

- Link

—

” “Wed, 17 Jul 2024

XenForo 2.2.15 Cross Site Request Forgery

XenForo versions 2.2.15 and below suffer from a cross site request forgery vulnerability in Widget::actionSave.

- Link

—

” “Wed, 17 Jul 2024

Hospital Management System Project In ASP.Net MVC 1 SQL Injection

Hospital Management System Project in ASP.Net MVC version 1 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Wed, 17 Jul 2024

Bonjour Service 3,0,0,10 Unquoted Service Path

Bonjour Service version 3,0,0,10 suffers from an unquoted service path vulnerability.

- Link

—

” “Mon, 15 Jul 2024

Geoserver Unauthenticated Remote Code Execution

GeoServer is an open-source software server written in Java that provides the ability to view, edit, and share geospatial data. It is designed to be a flexible, efficient solution for distributing geospatial data from a variety of sources such as Geographic Information System (GIS) databases, web-based data, and personal datasets. In the GeoServer versions before 2.23.6, greater than or equal to 2.24.0, before 2.24.4 and greater than equal to 2.25.0, and before 2.25.1, multiple OGC request parameters allow remote code execution (RCE) by unauthenticated users through specially crafted input against a default GeoServer installation due to unsafely evaluating property names as XPath expressions. An attacker can abuse this by sending a POST request with a malicious xpath expression to execute arbitrary commands as root on the system.

- Link

—

” “Mon, 15 Jul 2024

WordPress PZ Frontend Manager 1.0.5 Cross Site Request Forgery

WordPress PZ Frontend Manager plugin versions 1.0.5 and below suffer from a cross site request forgery vulnerability in the change user profile picture functionality.

- Link

—

” “Mon, 15 Jul 2024

Havoc C2 0.7 Server-Side Request Forgery

Havoc C2 version 0.7 suffers from an unauthenticated server-side request forgery vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Tue, 23 Jul 2024

ZDI-24-957: (0Day) Comodo Internet Security Pro cmdagent Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 23 Jul 2024

ZDI-24-956: (0Day) Comodo Internet Security Pro cmdagent Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 23 Jul 2024

ZDI-24-955: (0Day) Comodo Internet Security Pro cmdagent Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 23 Jul 2024

ZDI-24-954: (0Day) Comodo Firewall Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 23 Jul 2024

ZDI-24-953: (0Day) Comodo Internet Security Pro Directory Traversal Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-952: Delta Electronics CNCSoft-G2 DPAX File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-951: Delta Electronics CNCSoft-G2 DPAX File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-950: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-949: Delta Electronics CNCSoft-G2 DPAX File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-948: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-947: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-946: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-945: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-944: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-943: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-942: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-941: Delta Electronics CNCSoft-G2 DPAX File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-940: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-939: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-938: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-937: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-936: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-935: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-934: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-933: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-932: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-931: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-930: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-929: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-928: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-927: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-926: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-925: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote

Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-924: Delta Electronics CNCSoft-G2 ALM File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-923: Delta Electronics CNCSoft-G2 ALM File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-922: Delta Electronics CNCSoft-G2 CMT File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-921: Delta Electronics CNCSoft-G2 ALM File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-920: Delta Electronics CNCSoft-G2 ALM File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-919: Delta Electronics CNCSoft-G2 ALM File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-918: Delta Electronics CNCSoft-G2 ALM File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 22 Jul 2024

ZDI-24-917: Delta Electronics CNCSoft-G2 ALM File Parsing Stack-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: (Jul)

Datum	Opfer	Land	Information
2024-07-23	Red Art Games	[FRA]	Link
2024-07-22	Aéroport de Split	[HRV]	Link
2024-07-19	Le Tribunal supérieur du comté de Los Angeles	[USA]	Link
2024-07-18	Cadastre hellénique	[GRC]	Link
2024-07-18	Casino du Grand Cercle	[FRA]	Link
2024-07-18	Globes	[ISR]	Link
2024-07-17	Ingemmet	[PER]	Link
2024-07-16	Le Département de Loire-Atlantique	[FRA]	Link
2024-07-16	Les Transports Publics du Chablais (TPC)	[CHE]	Link
2024-07-15	Department of Migrant Workers (DMW)	[PHL]	Link
2024-07-15	Cadre Holdings, Inc.	[USA]	Link
2024-07-14	Metalfrio	[BRA]	Link
2024-07-14	MERB	[DEU]	Link
2024-07-13	AKG	[DEU]	Link
2024-07-12	Sesc Tocantins	[BRA]	Link
2024-07-12	ValeCard	[BRA]	Link
2024-07-11	Allegheny County District Attorney’s Office	[USA]	Link
2024-07-11	Solutions&Co	[FRA]	Link
2024-07-10	Jaboatão dos Guararapes	[BRA]	Link
2024-07-10	Sibanye Stillwater	[ZAF]	Link
2024-07-10	District scolaire de Goshen	[USA]	Link
2024-07-10	Bassett Furniture Industries Inc.	[USA]	Link
2024-07-10	Active Learning Trust	[GBR]	Link
2024-07-09	Clay County Courthouse	[USA]	Link
2024-07-09	Ville de Mahina	[FRA]	Link

Datum	Opfer	Land	Information
2024-07-07	Frankfurter University of Applied Sciences (UAS)	[DEU]	Link
2024-07-04	La Ville d'Ans	[BEL]	Link
2024-07-03	E.S.E. Salud Yopal	[COL]	Link
2024-07-03	Florida Department of Health	[USA]	Link
2024-07-03	Southwest Tennessee Community College (SWTCC)	[USA]	Link
2024-07-02	Hong Kong Institute of Architects	[HKG]	Link
2024-07-02	Apex	[USA]	Link
2024-07-01	Hiap Seng Industries	[SGP]	Link
2024-07-01	Monroe County government	[USA]	Link

7 Ransomware-Erpressungen: (Jul)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-24	[RhinoCorps]	blacksuit	Link
2024-07-17	[Congoleum]	play	Link
2024-07-23	[sigmacontrol.eu]	ransomhub	Link
2024-07-23	[siParadigm]	akira	Link
2024-07-23	[eurovilla.hr]	darkvault	Link
2024-07-23	[Notarkammer Pfalz]	akira	Link
2024-07-23	[Win Systems]	akira	Link
2024-07-20	[www.byzan.com]	ransomhub	Link
2024-07-16	[maingroup]	incransom	Link
2024-07-08	[Cedar Technologies]	medusa	Link
2024-07-12	[American Golf]	medusa	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-15	[Royal Brighton Yacht Club]	medusa	Link
2024-07-15	[ValeCard]	medusa	Link
2024-07-16	[H&H Group]	medusa	Link
2024-07-16	[Jariet Technologies]	medusa	Link
2024-07-22	[Globes]	medusa	Link
2024-07-22	[AA Munro Insurance]	medusa	Link
2024-07-23	[thesourcinggroup.com]	dAn0n	Link
2024-07-23	[LawDepot]	rhysida	Link
2024-07-23	[Association Management Strategies(AAMC.local)]	incransom	Link
2024-07-08	[CIMP.COM]	incransom	Link
2024-07-22	[Wichita State University Campus of Applied Sciences and Technology]	fog	Link
2024-07-22	[memc.com]	blackbasta	Link
2024-07-22	[SH Pension]	everest	Link
2024-07-11	[Sibanye-Stillwater]	ransomhouse	Link
2024-07-22	[Acadian Ambulance (US)]	daixin	Link
2024-07-21	[Sherbrooke Metals]	BrainCipher	Link
2024-07-21	[Apex Global	Big leak outlooks - 2tb.]	BrainCipher
2024-07-21	[Cole Technologies Group]	BrainCipher	Link
2024-07-21	[Family Wealth Advisors Ltd.]	BrainCipher	Link
2024-07-21	[Mars 2 LLC]	BrainCipher	Link
2024-07-21	[KickDown ESET company. No overpayments at 0% (renamed and update)]	donutleaks	Link
2024-07-21	[Handala’s attack on Israeli organizations]	handala	Link
2024-07-20	[Queens County Public Administrator]	rhysida	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-20	[www.garudafood.com]	ransomhub	Link
2024-07-20	[Reward Hospitality from EFC Group]	blacksuit	Link
2024-07-20	[ESET. PREMIUM.]	donutleaks	Link
2024-07-20	[Doodle Tech]	arcusmedia	Link
2024-07-19	[www.kumagaigumi.co.jp]	ransomhub	Link
2024-07-19	[Arcmed Group]	hunters	Link
2024-07-19	[Leech Lake Gaming]	cicada3301	Link
2024-07-15	[concorddirect.com]	lockbit3	Link
2024-07-15	[townandforest.co.uk]	lockbit3	Link
2024-07-17	[norton.k12.ma.us]	lockbit3	Link
2024-07-17	[energateinc.com]	lockbit3	Link
2024-07-17	[plantmachineworks.com]	lockbit3	Link
2024-07-17	[piedmonthoist.com]	lockbit3	Link
2024-07-17	[gptchb.org]	lockbit3	Link
2024-07-17	[assih.com]	lockbit3	Link
2024-07-18	[wattlerange.sa.gov.au]	lockbit3	Link
2024-07-18	[claycountyin.gov]	lockbit3	Link
2024-07-18	[iteam.gr]	lockbit3	Link
2024-07-18	[albonanova.at]	lockbit3	Link
2024-07-18	[lothar-rapp.de]	lockbit3	Link
2024-07-18	[goldstarmetal.com]	lockbit3	Link
2024-07-18	[glsco.com]	lockbit3	Link
2024-07-18	[paysdelaloire.fr]	lockbit3	Link
2024-07-18	[troyareasd.org]	lockbit3	Link
2024-07-18	[barkingwell.gr]	lockbit3	Link
2024-07-18	[fbrlaw.com]	lockbit3	Link
2024-07-18	[customssupport.be]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-18	[joliet86.org]	lockbit3	Link
2024-07-16	[www.glowfm.nl]	ransomhub	Link
2024-07-19	[Law Offices of the Public Defender - New Mexico]	rhysida	Link
2024-07-05	[Infomedika]	ransomhouse	Link
2024-07-17	[Next step healthcar]	qilin	Link
2024-07-18	[Northeast Rehabilitation Hospital Network]	hunters	Link
2024-07-18	[Seamon Whiteside]	hunters	Link
2024-07-18	[Santa Rosa]	hunters	Link
2024-07-18	[all-mode.com]	donutleaks	Link
2024-07-14	[www.erma-rtmo.it]	ransomhub	Link
2024-07-16	[metalfrio.com.br]	ransomhub	Link
2024-07-16	[www.newcastlewa.gov]	ransomhub	Link
2024-07-18	[pgd.pl]	ransomhub	Link
2024-07-17	[Modernauto]	blackbyte	Link
2024-07-17	[Modern Automotive Group]	blackbyte	Link
2024-07-17	[Gandara Center]	rhysida	Link
2024-07-17	[C???o???m]	play	Link
2024-07-17	[Hayden Power Group]	play	Link
2024-07-17	[MIPS Technologies]	play	Link
2024-07-17	[ZSZAALEJI.cz]	qilin	Link
2024-07-17	[Eyal Baror the key official of the 8200 unit]	handala	Link
2024-07-17	[labline.it]	donutleaks	Link
2024-07-16	[www.hlbpr.com]	ransomhub	Link
2024-07-17	[isometrix.com]	cactus	Link
2024-07-06	[A.L.P. Lighting Components]	incransom	Link
2024-07-16	[VITALDENT]	madliberator	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-12	[MINISTERO DELLA CULTURA]	madliberator	Link
2024-07-12	[MONTERO & SEGURA]	madliberator	Link
2024-07-12	[CROSSWEAR TRADING LTD]	madliberator	Link
2024-07-12	[Cities Network]	madliberator	Link
2024-07-17	[ZB Financial Holdings]	madliberator	Link
2024-07-17	[The Law Office of Omar O. Vargas, P.C.]	everest	Link
2024-07-17	[STUDIO NOTARILE BUCCI – OLMI]	everest	Link
2024-07-16	[GroupePRO-B]	cicada3301	Link
2024-07-16	[Greenheck]	meow	Link
2024-07-16	[CBIZ Inc]	meow	Link
2024-07-16	[Hewlett Packard Enterprise]	meow	Link
2024-07-16	[BCS Systems]	meow	Link
2024-07-16	[Guhring]	meow	Link
2024-07-16	[Odfjell Drilling]	meow	Link
2024-07-16	[Golan Christie Taglia]	meow	Link
2024-07-16	[First Commonwealth Federal Credit Union]	meow	Link
2024-07-07	[Djg Projects]	fog	Link
2024-07-04	[Verweij Elektrotechniek]	fog	Link
2024-07-04	[Alvin Independent School District]	fog	Link
2024-07-11	[West Allis-West Milwaukee School District]	fog	Link
2024-07-16	[German University of Technology in Oman]	fog	Link
2024-07-16	[ceopag.com.br / ceofood.com.br]	ransomhub	Link
2024-07-16	[[temporary] Warning for Eyal Baror]	handala	Link
2024-07-16	[www.benchinternational.com]	ransomhub	Link
2024-07-16	[www.cameronhodges.com]	ransomhub	Link
2024-07-16	[Braum’s Inc]	hunters	Link
2024-07-16	[Lantronix Inc.]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-16	[HOYA Corporation]	hunters	Link
2024-07-16	[Mainland Machinery]	dragonforce	Link
2024-07-16	[SBRPCA]	dragonforce	Link
2024-07-16	[verco.co.uk]	cactus	Link
2024-07-15	[Nuevatel]	dunghill	Link
2024-07-15	[Innovalve Bio Medical]	handala	Link
2024-07-09	[www.baiminstitute.org]	ransomhub	Link
2024-07-13	[integraservices]	mallox	Link
2024-07-14	[XENAPP-GLOBER]	mallox	Link
2024-07-15	[Gramercy Surgery Center]	everest	Link
2024-07-15	[posiplus.com]	blackbasta	Link
2024-07-15	[hpecds.com]	blackbasta	Link
2024-07-15	[Amino Transport]	akira	Link
2024-07-15	[Goede, DeBoest & Cross, PLLC.]	rhysida	Link
2024-07-15	[Sheba Medical Center]	handala	Link
2024-07-15	[usdermpartners.com]	blackbasta	Link
2024-07-15	[atos.com]	blackbasta	Link
2024-07-15	[Gibbs Hurley Chartered Accountants]	hunters	Link
2024-07-15	[ComNet Communications]	hunters	Link
2024-07-15	[MS Ultrasonic Technology Group]	hunters	Link
2024-07-15	[RZO]	hunters	Link
2024-07-15	[thompsoncreek.com_wa]	blackbasta	Link
2024-07-15	[northernsafety.com_wa]	blackbasta	Link
2024-07-15	[upcli.com]	cloak	Link
2024-07-15	[greenlightbiosciences.com]	abyss	Link
2024-07-15	[valleylandtitleco.com - UPD]	donutleaks	Link
2024-07-14	[luzan5.com]	blackout	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-14	[BrownWinick]	rhysida	Link
2024-07-14	[Texas Alcohol & Drug Testing Service]	bianlian	Link
2024-07-13	[a-g.com - data publication 38gb (150K)]	blacksuit	Link
2024-07-13	[gbhs.org Publication 51gb]	blacksuit	Link
2024-07-13	[Kenya Urban Roads Authority]	hunters	Link
2024-07-13	[Carigali Hess Operating Company]	hunters	Link
2024-07-13	[gbhs.org 07/12 Publication 51gb]	blacksuit	Link
2024-07-01	[The Coffee Bean & Tea Leaf]	incransom	Link
2024-07-01	[State of Alabama - Alabama Department Of Education]	incransom	Link
2024-07-02	[ARISTA]	spacebears	Link
2024-07-12	[Preferred IT Group]	bianlian	Link
2024-07-08	[Wagner-Meinert]	ransomexx	Link
2024-07-12	[painproclinics.com]	ransomcortex	Link
2024-07-02	[www.zepter.de]	ransomhub	Link
2024-07-11	[www.riteaid.com]	ransomhub	Link
2024-07-03	[olympusgrp.com]	dispossessor	Link
2024-07-12	[www.donaanita.com]	ransomcortex	Link
2024-07-12	[perfeitaplastica.com.br]	ransomcortex	Link
2024-07-12	[www.respirarlondrina.com.br]	ransomcortex	Link
2024-07-11	[Hyperice]	play	Link
2024-07-11	[diligentusa.com]	embargo	Link
2024-07-11	[Image Microsystems]	blacksuit	Link
2024-07-11	[www.lynchaluminum.com]	ransomhub	Link
2024-07-11	[www.eurostrand.de]	ransomhub	Link
2024-07-11	[www.netavent.dk]	ransomhub	Link
2024-07-11	[Financoop]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-11	[Sigma]	akira	Link
2024-07-11	[Sonol (Gas Stations)]	handala	Link
2024-07-11	[www.bfcsolutions.com]	ransomhub	Link
2024-07-11	[Texas Electric Cooperatives]	play	Link
2024-07-11	[The 21st Century Energy Group]	play	Link
2024-07-11	[T P C I]	play	Link
2024-07-10	[City of Cedar Falls]	blacksuit	Link
2024-07-10	[P448]	akira	Link
2024-07-10	[Beowulfchain]	vanirgroup	Link
2024-07-10	[Qinao]	vanirgroup	Link
2024-07-10	[Athlon]	vanirgroup	Link
2024-07-10	[Usina Alta Mogiana S/A]	akira	Link
2024-07-09	[Inland Audio Visual]	akira	Link
2024-07-09	[Indika Energy]	hunters	Link
2024-07-08	[Excelsior Orthopaedics]	monti	Link
2024-07-09	[Heidmar]	akira	Link
2024-07-03	[REPLIGEN]	incransom	Link
2024-07-08	[Raffmetal Spa]	dragonforce	Link
2024-07-08	[Allied Industrial Group]	akira	Link
2024-07-08	[Esedra]	akira	Link
2024-07-08	[Federated Co-operatives]	akira	Link
2024-07-02	[Guhring USA]	incransom	Link
2024-07-06	[noab.nl]	lockbit3	Link
2024-07-07	[Strauss Brands]	medusa	Link
2024-07-07	[Harry Perkins Institute of medical research]	medusa	Link
2024-07-07	[Viasat]	medusa	Link
2024-07-07	[Olympus Group]	medusa	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-07	[MYC Media]	rhysida	Link
2024-07-06	[a-g.com 7/10/24 - data publication 38gb (150K)]	blacksuit	Link
2024-07-03	[baiminstitute.org]	ransomhub	Link
2024-07-05	[The Wacks Law Group]	qilin	Link
2024-07-05	[pomalca.com.pe]	qilin	Link
2024-07-05	[Center for Human Capital Innovation (centerforhci.org)]	incransom	Link
2024-07-05	[waupacacounty-wi.gov]	incransom	Link
2024-07-05	[waupaca.wi.us]	incransom	Link
2024-07-04	[ws-stahl.eu]	lockbit3	Link
2024-07-04	[homelandvinyl.com]	lockbit3	Link
2024-07-04	[eicher.in]	lockbit3	Link
2024-07-05	[National Health Laboratory Services]	blacksuit	Link
2024-07-04	[Un Museau]	spacebears	Link
2024-07-03	[Haylem]	spacebears	Link
2024-07-04	[Elyria Foundry]	play	Link
2024-07-04	[Texas Recycling]	play	Link
2024-07-04	[INDA’s]	play	Link
2024-07-04	[Innerspec Technologies]	play	Link
2024-07-04	[Prairie Athletic Club]	play	Link
2024-07-04	[Fareri Associates]	play	Link
2024-07-04	[Island Transportation Corp.]	bianlian	Link
2024-07-04	[Legend Properties, Inc.]	bianlian	Link
2024-07-04	[Transit Mutual Insurance Corporation]	bianlian	Link
2024-07-03	[hcri.edu]	ransomhub	Link
2024-07-04	[Coquitlam Concrete]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-04	[Multisuns Communication]	hunters	Link
2024-07-04	[gerard-perrier.com]	embargo	Link
2024-07-04	[Abileneisd.org]	cloak	Link
2024-07-03	[sequelglobal.com]	darkvault	Link
2024-07-03	[Explomin]	akira	Link
2024-07-03	[Alimac]	akira	Link
2024-07-03	[badel1862.hr]	blackout	Link
2024-07-03	[ramservices.com]	underground	Link
2024-07-03	[foremedia.net]	darkvault	Link
2024-07-03	[www.swcs-inc.com]	ransomhub	Link
2024-07-03	[valleylandtitleco.com]	donutleaks	Link
2024-07-02	[merrymanhouse.org]	lockbit3	Link
2024-07-02	[fairfieldmemorial.org]	lockbit3	Link
2024-07-02	[www.daesangamerica.com]	ransomhub	Link
2024-07-02	[P1 Technologies]	akira	Link
2024-07-02	[Conexus Medstaff]	akira	Link
2024-07-02	[Salton]	akira	Link
2024-07-01	[www.sfmedical.de]	ransomhub	Link
2024-07-02	[WheelerShip]	hunters	Link
2024-07-02	[Grand Rapids Gravel]	dragonforce	Link
2024-07-02	[Franciscan Friars of the Atonement]	dragonforce	Link
2024-07-02	[Elite Fitness]	dragonforce	Link
2024-07-02	[Gray & Adams]	dragonforce	Link
2024-07-02	[Vermont Panurgy]	dragonforce	Link
2024-07-01	[floridahealth.gov]	ransomhub	Link
2024-07-01	[www.nttdata.ro]	ransomhub	Link
2024-07-01	[Super Gardens]	dragonforce	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-01	[Hampden Veterinary Hospital]	dragonforce	Link
2024-07-01	[Indonesia Terkoneksi]	BrainCipher	Link
2024-07-01	[SYNERGY PEANUT]	akira	Link
2024-07-01	[Ethypharm]	underground	Link
2024-07-01	[latinusa.co.id]	lockbit3	Link
2024-07-01	[kbc-zagreb.hr]	lockbit3	Link
2024-07-01	[maxcess-logistics.com]	killsec	Link
2024-07-01	[Independent Education System]	handala	Link
2024-07-01	[Bartlett & Weigle Co. LPA.]	hunters	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.