Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240725

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

Siemens SICAM: Angreifer können Admin-Passwort zurücksetzen

SCADA-Systeme der SICAM-Reihe von Siemens kommen in kritischen Infrastrukturen zum Einsatz. Sicherheitsupdates schließen eine kritische Lücke.

- Link

—

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

—

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	0.988550000	Link
CVE-2023-6895	0.922010000	0.989950000	Link
CVE-2023-6553	0.937510000	0.991560000	Link
CVE-2023-5360	0.903980000	0.988610000	Link
CVE-2023-52251	0.938200000	0.991650000	Link
CVE-2023-4966	0.971710000	0.998310000	Link
CVE-2023-49103	0.953130000	0.993860000	Link
CVE-2023-48795	0.965740000	0.996420000	Link
CVE-2023-47246	0.948140000	0.993020000	Link
CVE-2023-46805	0.958670000	0.994820000	Link
CVE-2023-46747	0.972730000	0.998710000	Link
CVE-2023-46604	0.963510000	0.995820000	Link
CVE-2023-4542	0.921170000	0.989830000	Link
CVE-2023-43208	0.964870000	0.996130000	Link
CVE-2023-43177	0.962660000	0.995610000	Link
CVE-2023-42793	0.970960000	0.998040000	Link
CVE-2023-41265	0.905890000	0.988720000	Link
CVE-2023-39143	0.938190000	0.991640000	Link
CVE-2023-38646	0.910550000	0.989030000	Link
CVE-2023-38205	0.954590000	0.994140000	Link
CVE-2023-38203	0.966000000	0.996470000	Link
CVE-2023-38146	0.915710000	0.989370000	Link
CVE-2023-38035	0.974400000	0.999560000	Link
CVE-2023-36845	0.961840000	0.995440000	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	0.990750000	Link
CVE-2023-34634	0.927960000	0.990560000	Link
CVE-2023-34468	0.906650000	0.988800000	Link
CVE-2023-34362	0.969450000	0.997490000	Link
CVE-2023-34039	0.940490000	0.991910000	Link
CVE-2023-3368	0.933870000	0.991200000	Link
CVE-2023-33246	0.972610000	0.998660000	Link
CVE-2023-32315	0.973620000	0.999130000	Link
CVE-2023-30625	0.948260000	0.993050000	Link
CVE-2023-30013	0.962250000	0.995510000	Link
CVE-2023-29300	0.968930000	0.997330000	Link
CVE-2023-29298	0.943640000	0.992330000	Link
CVE-2023-28771	0.902140000	0.988480000	Link
CVE-2023-28343	0.949510000	0.993220000	Link
CVE-2023-28121	0.909760000	0.988970000	Link
CVE-2023-27524	0.970300000	0.997800000	Link
CVE-2023-27372	0.972890000	0.998790000	Link
CVE-2023-27350	0.970130000	0.997730000	Link
CVE-2023-26469	0.951490000	0.993540000	Link
CVE-2023-26360	0.959350000	0.994960000	Link
CVE-2023-26035	0.967100000	0.996800000	Link
CVE-2023-25717	0.956860000	0.994520000	Link
CVE-2023-25194	0.968820000	0.997320000	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	0.995030000	Link
CVE-2023-22527	0.970550000	0.997890000	Link
CVE-2023-22518	0.964890000	0.996130000	Link
CVE-2023-22515	0.973590000	0.999120000	Link
CVE-2023-21839	0.957210000	0.994580000	Link
CVE-2023-21554	0.952830000	0.993790000	Link
CVE-2023-20887	0.970170000	0.997740000	Link
CVE-2023-1698	0.910560000	0.989040000	Link
CVE-2023-1671	0.962480000	0.995570000	Link
CVE-2023-0669	0.969440000	0.997480000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 24 Jul 2024

[NEU] [hoch] docker: Schwachstelle ermöglicht Privilegieneskalation

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

- Link

—

Wed, 24 Jul 2024

[NEU] [hoch] Aruba EdgeConnect: Mehrere Schwachstellen

Ein entfernter authentifizierter Angreifer kann mehrere Schwachstellen in Aruba EdgeConnect ausnutzen, um beliebigen Code auszuführen oder einen Cross-Site-Scripting-Angriff durchzuführen.

- Link

—

Wed, 24 Jul 2024

[NEU] [hoch] SolarWinds Platform: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in SolarWinds Platform ausnutzen,

um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu erzeugen, Daten zu manipulieren und vertrauliche Informationen preiszugeben.

- Link

—

Wed, 24 Jul 2024

[NEU] [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, 24 Jul 2024

[UPDATE] [hoch] Apache ActiveMQ: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache ActiveMQ ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 24 Jul 2024

[UPDATE] [hoch] Apache Tomcat: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache Tomcat ausnutzen, um Informationen offenzulegen oder beliebigen Programmcode auszuführen.

- Link

—

Wed, 24 Jul 2024

[UPDATE] [kritisch] Apache ActiveMQ: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache ActiveMQ ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 24 Jul 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

—

Wed, 24 Jul 2024

[UPDATE] [hoch] Apache ActiveMQ: Schwachstelle ermöglicht Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Apache ActiveMQ ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 24 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

—

Wed, 24 Jul 2024

[UPDATE] [hoch] EDK2 NetworkPkg IP stack implementation: Mehrere Schwachstellen

Ein Angreifer aus dem angrenzenden Netzwerk oder ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der EDK2 NetworkPkg IP stack implementation ausnutzen, um beliebigen Programmcode auszuführen, vertrauliche Informationen offenzulegen und einen Denial of Service Zustand auszulösen.

- Link

—

Wed, 24 Jul 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder seine Privilegien zu erweitern.

- Link

—

Wed, 24 Jul 2024

[UPDATE] [hoch] LibreOffice: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in LibreOffice ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 24 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

—

Wed, 24 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

—

Wed, 24 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

—

Wed, 24 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

—

Wed, 24 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] 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

[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

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
7/24/2024	[Photon OS 3.0: Strongswan PHSA-2023-3.0-0694]	critical
7/24/2024	[Photon OS 3.0: Bluez PHSA-2023-3.0-0570]	critical
7/24/2024	[Photon OS 5.0: Httpd PHSA-2024-5.0-0330]	critical
7/24/2024	[Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2024-12548)]	critical
7/24/2024	[Oracle Linux 8 : Unbreakable Enterprise kernel-container (ELSA-2024-12552)]	critical
7/24/2024	[Oracle Linux 7 / 8 : Unbreakable Enterprise kernel (ELSA-2024-12547)]	critical
7/24/2024	[Oracle Linux 7 : Unbreakable Enterprise kernel-container (ELSA-2024-12551)]	critical
7/24/2024	[Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2024-12549)]	critical
7/24/2024	[Photon OS 3.0: Nginx PHSA-2022-3.0-0481]	high
7/24/2024	[Photon OS 3.0: Cyrus PHSA-2022-3.0-0368]	high
7/24/2024	[Photon OS 3.0: Vim PHSA-2023-3.0-0671]	high
7/24/2024	[Photon OS 3.0: Go PHSA-2022-3.0-0455]	high
7/24/2024	[Photon OS 3.0: Squid PHSA-2024-3.0-0707]	high
7/24/2024	[Photon OS 5.0: Suricata PHSA-2024-5.0-0326]	high
7/24/2024	[Photon OS 3.0: Freetype2 PHSA-2022-3.0-0394]	high
7/24/2024	[Photon OS 3.0: Sendmail PHSA-2022-3.0-0382]	high
7/24/2024	[Photon OS 3.0: Open PHSA-2023-3.0-0675]	high
7/24/2024	[Photon OS 3.0: Ruby PHSA-2022-3.0-0447]	high

Datum	Schwachstelle	Bewertung
7/24/2024	[Photon OS 3.0: Uriparser PHSA-2024-3.0-0772]	high
7/24/2024	[Photon OS 3.0: Device PHSA-2022-3.0-0476]	high
7/24/2024	[Photon OS 3.0: Zchunk PHSA-2023-3.0-0683]	high
7/24/2024	[Photon OS 3.0: Grub2 PHSA-2023-3.0-0643]	high
7/24/2024	[Photon OS 5.0: Bindutils PHSA-2024-5.0-0330]	high
7/24/2024	[Photon OS 3.0: Netkit PHSA-2023-3.0-0665]	high
7/24/2024	[Photon OS 4.0: Bindutils PHSA-2024-4.0-0657]	high
7/24/2024	[Photon OS 3.0: Binutils PHSA-2023-3.0-0643]	high
7/24/2024	[Photon OS 4.0: Curl PHSA-2024-4.0-0658]	high
7/24/2024	[Photon OS 5.0: Curl PHSA-2024-5.0-0328]	high
7/24/2024	[Ubuntu 22.04 LTS / 24.04 LTS : poppler vulnerability (USN-6915-1)]	high
7/24/2024	[Ubuntu 20.04 LTS / 22.04 LTS : phpCAS vulnerability (USN-6913-1)]	high
7/24/2024	[Ubuntu 22.04 LTS : OCS Inventory vulnerability (USN-6914-1)]	high
7/24/2024	[Oracle Linux 9 : edk2 (ELSA-2024-4749)]	high
7/24/2024	[GitLab 16.6 < 17.0.5 / 17.1 < 17.1.3 / 17.2 < 17.2.1 (CVE-2024-7047)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Wed, 24 Jul 2024

SIM Wisuda 1.0 Insecure Direct Object Reference

SIM Wisuda version 1.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Wed, 24 Jul 2024

SLiMS CMS 2.0 SQL Injection

SLiMS CMS version 2.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Wed, 24 Jul 2024

StarTask CRM 1.9 SQL Injection

StarTask CRM version 1.9 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Wed, 24 Jul 2024

UBM CMS 1.2 Insecure Direct Object Reference

UBM CMS version 1.2 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Wed, 24 Jul 2024

TAIF LMS 5.8.0 Shell Upload

TAIF LMS version 5.8.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Wed, 24 Jul 2024

Vencorp 2.1.1 SQL Injection

Vencorp version 2.1.1 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Wed, 24 Jul 2024

Webdenim AppUI 1.0 Insecure Direct Object Reference

Webdenim AppUI version 1.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “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

—

”

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
2024-07-23	Ville de Cold Lake	[CAN]	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
2024-07-18	Ville de Columbus	[USA]	Link
2024-07-18	Wattle Range Council	[AUS]	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

Datum	Opfer	Land	Information
2024-07-10	Active Learning Trust	[GBR]	Link
2024-07-09	Clay County Courthouse	[USA]	Link
2024-07-09	Ville de Mahina	[FRA]	Link
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	[Stienemann]	spacebears	Link
2024-07-25	[Pojoaque]	blacksuit	Link
2024-07-24	[Kusum Group of Companies]	raworld	Link
2024-07-24	[TheLutheranFoundation]	raworld	Link
2024-07-24	[Melchers Singapore]	raworld	Link
2024-07-20	[Valisana]	ransomhouse	Link
2024-07-24	[simple-solution-systems]	qilin	Link
2024-07-24	[Bunkhouse Group]	bianlian	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-24	[Playa Vista Job Opportunities and Business Services]	bianlian	Link
2024-07-24	[Accelon Technologies Private]	bianlian	Link
2024-07-24	[SKC West]	akira	Link
2024-07-24	[ORBINOX]	madliberator	Link
2024-07-24	[Uw logistieke partner]	madliberator	Link
2024-07-24	[Betances Health Center]	hunters	Link
2024-07-23	[BLEnergy]	handala	Link
2024-07-24	[Jack “Designer” Sparrow.]	donutleaks	Link
2024-07-24	[American Acryl]	akira	Link
2024-07-24	[Electroalfa]	akira	Link
2024-07-24	[CALDAN Conveyor]	akira	Link
2024-07-24	[forestparkga.gov]	monti	Link
2024-07-24	[Regas (regasenergy.com)]	monti	Link
2024-07-24	[Dimbleby Funeral Homes]	dragonforce	Link
2024-07-24	[John Gallin & Son]	dragonforce	Link
2024-07-24	[Industrial Bolsera]	donutleaks	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-12	[American Golf]	medusa	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-20	[Queens County Public Administrator]	rhysida	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-18	[customssupport.be]	lockbit3	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-16	[VITALDENT]	madliberator	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-16	[Lantronix Inc.]	hunters	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-14	[luzan5.com]	blackout	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-11	[Financoop]	akira	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-07	[Olympus Group]	medusa	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-04	[Coquitlam Concrete]	hunters	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-01	[Super Gardens]	dragonforce	Link
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.