Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241212

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

Solarwinds Web Help Desk: Software-Update schließt kritische Lücken

In Solarwinds Web Help Desk haben die Entwickler teils kritische Sicherheitslücken korrigiert. IT-Verantwortliche sollten rasch aktualisieren.

- Link

—

Patchday: Adobe schließt mehr als 160 Sicherheitslücken in Acrobat & Co.

Mehrere Schwachstellen in Anwendungen von Adobe können als Einfallstor für Angreifer dienen. Sicherheitsupdates stehen bereit.

- Link

—

Patchday: Angreifer attackieren Windows und verschaffen sich System-Rechte

Microsoft hat wichtige Sicherheitsupdates für unter anderem Hyper-V, Office, Share Point und Windows veröffentlicht. Eine Lücke wird bereits ausgenutzt.

- Link

—

Ivanti patcht zahlreiche Produkte

Ivanti hat Updates für mehrere Produkte veröffentlicht. Die Softwareflicken schließen teils kritische Sicherheitslücken.

- Link

—

Transfer-Software von Cleo: Hinter Firewall bringen, Patch wirkungslos

Die Datenstransfer-Software von Cleo hatte eine Sicherheitslücke gestopft – jedoch unzureichend. Das Leck wird aktiv angegriffen.

- Link

—

IBM App Connect Enterprise Certified Container mit Schadcode-Lücke

In aktuellen Versionen haben IBM-Entwickler in App Connect Enterprise Certified Container eine Schwachstelle geschlossen.

- Link

—

OpenWrt: Angreifer hätten bestimmte Images mit Schadcode verseuchen können

Aufgrund eines Fehlers hätten mit Schadcode präparierte OpenWrt-Images in Umlauf kommen können. Mittlerweile ist das Sicherheitsproblem gelöst.

- Link

—

SAP-Patchday: Updates schließen teils kritische Sicherheitslücken

Im Dezember informiert SAP über neun neu entdeckte Sicherheitslücken in diversen Produkten. Eine davon gilt als kritisches Risiko.

- Link

—

Wordpress: WPForms-Plug-in reißt Sicherheitsleck in 6 Millionen Webseiten

Im Wordpress-Plug-in WPForms können Angreifer eine Lücke missbrauchen, um etwa Zahlungen rückabzuwickeln. Sechs Millionen Webseiten nutzen das Plug-in.

- Link

—

Sicherheitsupdates: Angreifer können Qnap NAS kompromittieren

Netzwerkspeicher von Qnap sind verwundbar. Angreifer können an mehreren Schwachstellen ansetzen.

- 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	0.958030000	0.995210000	Link
CVE-2023-6895	0.936280000	0.992230000	Link
CVE-2023-6553	0.952340000	0.994280000	Link
CVE-2023-6019	0.935090000	0.992100000	Link
CVE-2023-6018	0.916750000	0.990490000	Link
CVE-2023-52251	0.949550000	0.993880000	Link
CVE-2023-4966	0.971030000	0.998310000	Link
CVE-2023-49103	0.949250000	0.993830000	Link
CVE-2023-48795	0.962800000	0.996030000	Link
CVE-2023-47246	0.963300000	0.996160000	Link
CVE-2023-46805	0.957820000	0.995150000	Link
CVE-2023-46747	0.973170000	0.999100000	Link
CVE-2023-46604	0.968210000	0.997440000	Link
CVE-2023-4542	0.941060000	0.992780000	Link
CVE-2023-43208	0.974210000	0.999560000	Link
CVE-2023-43177	0.959640000	0.995450000	Link
CVE-2023-42793	0.971260000	0.998380000	Link
CVE-2023-4220	0.948030000	0.993680000	Link
CVE-2023-41265	0.903830000	0.989550000	Link
CVE-2023-39143	0.920260000	0.990760000	Link
CVE-2023-38205	0.950620000	0.994030000	Link
CVE-2023-38203	0.964750000	0.996480000	Link
CVE-2023-38146	0.906640000	0.989740000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-38035	0.973670000	0.999290000	Link
CVE-2023-36845	0.967890000	0.997360000	Link
CVE-2023-3519	0.965540000	0.996690000	Link
CVE-2023-35082	0.961850000	0.995850000	Link
CVE-2023-35078	0.969720000	0.997860000	Link
CVE-2023-34993	0.972760000	0.998950000	Link
CVE-2023-34634	0.926130000	0.991190000	Link
CVE-2023-34362	0.970200000	0.998060000	Link
CVE-2023-34039	0.929610000	0.991530000	Link
CVE-2023-3368	0.938260000	0.992470000	Link
CVE-2023-33246	0.973150000	0.999080000	Link
CVE-2023-32315	0.973420000	0.999190000	Link
CVE-2023-32235	0.926990000	0.991280000	Link
CVE-2023-30625	0.950690000	0.994040000	Link
CVE-2023-30013	0.968110000	0.997410000	Link
CVE-2023-29300	0.968250000	0.997460000	Link
CVE-2023-29298	0.969330000	0.997750000	Link
CVE-2023-28432	0.906870000	0.989750000	Link
CVE-2023-28343	0.966250000	0.996870000	Link
CVE-2023-28121	0.929810000	0.991550000	Link
CVE-2023-27524	0.970390000	0.998100000	Link
CVE-2023-27372	0.973870000	0.999400000	Link
CVE-2023-27350	0.967700000	0.997330000	Link
CVE-2023-26469	0.957270000	0.995050000	Link
CVE-2023-26360	0.962010000	0.995900000	Link
CVE-2023-26035	0.968960000	0.997640000	Link
CVE-2023-25717	0.949440000	0.993840000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-25194	0.968460000	0.997520000	Link
CVE-2023-2479	0.963800000	0.996280000	Link
CVE-2023-24489	0.972870000	0.998970000	Link
CVE-2023-23752	0.948310000	0.993720000	Link
CVE-2023-23397	0.902750000	0.989490000	Link
CVE-2023-23333	0.963300000	0.996170000	Link
CVE-2023-22527	0.967990000	0.997380000	Link
CVE-2023-22518	0.963030000	0.996100000	Link
CVE-2023-22515	0.973360000	0.999160000	Link
CVE-2023-21839	0.922450000	0.990900000	Link
CVE-2023-21554	0.951950000	0.994210000	Link
CVE-2023-20887	0.968860000	0.997620000	Link
CVE-2023-1671	0.959710000	0.995470000	Link
CVE-2023-0669	0.972180000	0.998730000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 11 Dec 2024

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um einen Denial of Service Angriff durchzuführen und um Sicherheitsmechanismen zu umgehen.

- Link

—

Wed, 11 Dec 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

—

Wed, 11 Dec 2024

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

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

- Link

—

Wed, 11 Dec 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

—

Wed, 11 Dec 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

—

Wed, 11 Dec 2024

[UPDATE] [kritisch] PHP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um beliebigen Programmcode auszuführen, Informationen preiszugeben und andere nicht spezifizierte Angriffe durchzuführen.

- Link

—

Wed, 11 Dec 2024

[NEU] [hoch] Python “virtualenv”: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle im Python “virtualenv” Paket ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 11 Dec 2024

[NEU] [hoch] Ivanti Connect Secure und Policy Secure: Mehrere Schwachstellen ermöglichen Codeausführung

Ein Angreifer kann mehrere Schwachstellen in Ivanti Connect Secure und Ivanti Policy Secure ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmaßnahmen zu umgehen oder

einen Denial of Service zu verursachen.

- Link

—

Wed, 11 Dec 2024

[NEU] [hoch] Atlassian Confluence: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Atlassian Confluence ausnutzen, um einen Denial of Service Angriff durchzuführen, Daten zu manipulieren oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 11 Dec 2024

[NEU] [hoch] Adobe Creative Cloud Applikationen: Mehrere Schwachstellen

Ein Angreifer kann diese Schwachstellen ausnutzen, um beliebigen Code auszuführen, erhöhte Rechte zu erlangen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen preiszugeben und einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Wed, 11 Dec 2024

[NEU] [hoch] Splunk Splunk Enterprise: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Splunk Splunk Enterprise ausnutzen, um vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen oder unspezifische Angriffe durchzuführen.

- Link

—

Wed, 11 Dec 2024

[NEU] [hoch] Ivanti Sentry: Schwachstelle ermöglicht Manipulation von Dateien

Ein lokaler Angreifer kann eine Schwachstelle in Ivanti Sentry ausnutzen, um Dateien zu manipulieren.

- Link

—

Wed, 11 Dec 2024

[NEU] [hoch] Google Chrome: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Wed, 11 Dec 2024

[NEU] [hoch] Atlassian Bamboo: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Atlassian Bamboo ausnutzen, um Dateien zu manipulieren oder einen Denial-of-Service-Zustand zu erzeugen.
- Link

—

Wed, 11 Dec 2024

[NEU] [hoch] Apache Struts: Schwachstelle ermöglicht Codeausführung

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

—

Wed, 11 Dec 2024

[NEU] [kritisch] Microsoft Windows: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in verschiedenen Versionen von Microsoft Windows und Microsoft Windows Server ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen und einen Denial-of-Service-Situation zu erzeugen.
- Link

—

Wed, 11 Dec 2024

[NEU] [UNGEPATCHT] [hoch] Siemens SIMATIC S7: Mehrere Schwachstellen ermöglichen Codeausführung

Ein lokaler Angreifer kann mehrere Schwachstellen in Siemens SIMATIC S7 ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Wed, 11 Dec 2024

[NEU] [hoch] Ivanti Cloud Services Appliance: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Ivanti Cloud Services Appliance ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen und beliebige SQL-Anweisungen auszuführen.
- Link

—

Wed, 11 Dec 2024

[NEU] [hoch] Microsoft SystemCenter: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Microsoft SystemCenter und Microsoft Defender ausnutzen, um seine Privilegien zu erhöhen und einen Spoofing-Angriff durchzuführen.
- Link

—

Wed, 11 Dec 2024

[NEU] [hoch] Microsoft Muzic: Schwachstelle ermöglicht Codeausführung

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

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
12/12/2024	[SUSE SLES12 Security Update : glib2 (SUSE-SU-2024:4051-1)]	critical
12/12/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : python-virtualenv (SUSE-SU-2024:4093-1)]	critical
12/12/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaFirefox (SUSE-SU-2024:4086-1)]	critical
12/12/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaThunderbird (SUSE-SU-2024:4148-1)]	critical
12/12/2024	[SUSE SLES12 Security Update : kernel (SUSE-SU-2024:4100-1)]	critical
12/12/2024	[SUSE SLES15 / openSUSE 15 Security Update : php8 (SUSE-SU-2024:4136-1)]	critical
12/12/2024	[SUSE SLES12 Security Update : tomcat (SUSE-SU-2024:4075-1)]	critical
12/12/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : glib2 (SUSE-SU-2024:4078-1)]	critical
12/12/2024	[SUSE SLES15 / openSUSE 15 Security Update : frr (SUSE-SU-2024:4090-1)]	critical
12/12/2024	[SUSE SLES15 / openSUSE 15 Security Update : tomcat (SUSE-SU-2024:4106-1)]	critical

Datum	Schwachstelle	Bewertung
12/12/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : postgresql, postgresql16, postgresql17 (SUSE-SU-2024:4173-1)]	high
12/12/2024	[SUSE SLES15 Security Update : kernel (SUSE-SU-2024:4103-1)]	high
12/12/2024	[SUSE SLES15 / openSUSE 15 Security Update : postgresql14 (SUSE-SU-2024:4176-1)]	high
12/12/2024	[SUSE SLES15 / openSUSE 15 Security Update : postgresql13 (SUSE-SU-2024:4175-1)]	high
12/12/2024	[SUSE SLES15 Security Update : kernel RT (Live Patch 17 for SLE 15 SP5) (SUSE-SU-2024:4128-1)]	high
12/12/2024	[SUSE SLES15 / openSUSE 15 Security Update : postgresql15 (SUSE-SU-2024:4098-1)]	high
12/12/2024	[SUSE SLES15 Security Update : kernel RT (Live Patch 14 for SLE 15 SP5) (SUSE-SU-2024:4125-1)]	high
12/12/2024	[SUSE SLES12 Security Update : postgresql13 (SUSE-SU-2024:4114-1)]	high
12/12/2024	[SUSE SLES15 Security Update : webkit2gtk3 (SUSE-SU-2024:4167-1)]	high
12/12/2024	[SUSE SLES15 Security Update : SUSE Manager Salt Bundle (SUSE-SU-2024:4021-1)]	high
12/12/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : postgresql, postgresql16, postgresql17 (SUSE-SU-2024:4063-1)]	high
12/12/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : libuv (SUSE-SU-2024:4109-1)]	high
12/12/2024	[SUSE SLES15 / openSUSE 15 Security Update : php7 (SUSE-SU-2024:4146-1)]	high
12/12/2024	[SUSE SLES12 Security Update : postgresql15 (SUSE-SU-2024:4095-1)]	high

Datum	Schwachstelle	Bewertung
12/12/2024	[SUSE SLES15 Security Update : kernel (Live Patch 46 for SLE 15 SP3) (SUSE-SU-2024:4161-1)]	high
12/12/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaThunderbird (SUSE-SU-2024:4050-1)]	high
12/12/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : python-waitress (SUSE-SU-2024:4107-1)]	high
12/12/2024	[SUSE SLES15 / openSUSE 15 Security Update : govulncheck-vulndb (SUSE-SU-2024:4042-1)]	high
12/12/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : wireshark (SUSE-SU-2024:4142-1)]	high
12/12/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : python-tornado6 (SUSE-SU-2024:4137-1)]	high
12/12/2024	[SUSE SLES15 Security Update : kernel RT (Live Patch 13 for SLE 15 SP5) (SUSE-SU-2024:4124-1)]	high
12/12/2024	[SUSE SLES15 Security Update : kernel (Live Patch 44 for SLE 15 SP3) (SUSE-SU-2024:4180-1)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Tue, 03 Dec 2024

Acronis Cyber Protect/Backup Remote Code Execution

The Acronis Cyber Protect appliance, in its default configuration, allows the anonymous registration of new protect/backup agents on new endpoints. This API endpoint also generates bearer tokens which the agent then uses to authenticate to the appliance. As the management web console is running on the same port as the API for the agents, this bearer token is also valid for any actions on the web console. This allows an attacker with network access to the appliance to start the registration of a new agent, retrieve a bearer token that provides admin access to the available functions in the web console. The web console contains multiple possibilities to execute arbitrary commands on both the agents (e.g., via PreCommands for a backup) and also the appliance (e.g., via a Validation job on the agent of the appliance). These options can easily be set with the provided bearer token, which

leads to a complete compromise of all agents and the appliance itself.

- Link

—

” “Tue, 03 Dec 2024

Fortinet FortiManager Unauthenticated Remote Code Execution

This Metasploit module exploits a missing authentication vulnerability affecting FortiManager and FortiManager Cloud devices to achieve unauthenticated RCE with root privileges. The vulnerable FortiManager versions are 7.6.0, 7.4.0 through 7.4.4, 7.2.0 through 7.2.7, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, and 6.2.0 through 6.2.12. The vulnerable FortiManager Cloud versions are 7.4.1 through 7.4.4, 7.2.1 through 7.2.7, 7.0.1 through 7.0.12, and 6.4 (all versions).

- Link

—

” “Tue, 03 Dec 2024

Asterisk AMI Originate Authenticated Remote Code Execution

On Asterisk, prior to versions 18.24.2, 20.9.2, and 21.4.2 and certified-asterisk versions 18.9-cert11 and 20.7-cert2, an AMI user with write=originate may change all configuration files in the /etc/asterisk/ directory. Writing a new extension can be created which performs a system command to achieve RCE as the asterisk service user (typically asterisk). Default parking lot in FreePBX is called ”Default lot” on the website interface, however its actually parkedcalls. Tested against Asterisk 19.8.0 and 18.16.0 on Freepbx SNG7-PBX16-64bit-2302-1.

- Link

—

” “Mon, 02 Dec 2024

Omada Identity Cross Site Scripting

Omada Identity versions prior to 15U1 and 14.14 hotfix #309 suffer from a persistent cross site scripting vulnerability.

- Link

—

” “Mon, 02 Dec 2024

Siemens Unlocked JTAG Interface / Buffer Overflow

Various Siemens products suffer from vulnerabilities. There is an unlocked JTAG Interface for Zynq-7000 on SM-2558 and a buffer overflow on the webserver of the SM-2558, CP-2016, and CP-2019 systems.

- Link

—

” “Mon, 02 Dec 2024

ABB Cylon Aspect 3.08.00 fileSystemUpdate.php File Upload / Denial Of Service

ABB Cylon Aspect version 3.08.00 suffers from a vulnerability in the fileSystemUpdate.php endpoint

of the ABB BEMS controller due to improper handling of uploaded files. The endpoint lacks restrictions on file size and type, allowing attackers to upload excessively large or malicious files. This flaw could be exploited to cause denial of service (DoS) attacks, memory leaks, or buffer overflows, potentially leading to system crashes or further compromise.

- Link

—

” “Mon, 02 Dec 2024

ABB Cylon Aspect 3.08.01 mstpstatus.php Information Disclosure

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated information disclosure vulnerability. An unauthorized attacker can reference the affected page and disclose various BACnet MS/TP statistics running on the device.

- Link

—

” “Mon, 02 Dec 2024

ABB Cylon Aspect 3.08.01 diagLateThread.php Information Disclosure

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated information disclosure vulnerability. An unauthorized attacker can reference the affected page and disclose various protocol thread information running on the device.

- Link

—

” “Mon, 02 Dec 2024

AppleAVD AV1_Syntax::Parse_Header Out-Of-Bounds Reads

AppleAVD has an issue where a large OBU size in AV1_Syntax::Parse_Header reading can lead to out-of-bounds reads.

- Link

—

” “Mon, 02 Dec 2024

AppleAVD AV1_Syntax::f Out-Of-Bounds Reads

AppleAVD has an issue in AV1_Syntax::f leading to out-of-bounds reads.

- Link

—

” “Mon, 02 Dec 2024

AppleAVD AV1_Syntax::Parse_Header Integer Underflow / Out-Of-Bounds Reads

AppleAVD has an integer underflow in AV1_Syntax::Parse_Header that can lead to out-of-bounds reads.

- Link

—

” “Mon, 02 Dec 2024

Simple Chat System 1.0 Cross Site Scripting

Simple Chat System version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 02 Dec 2024

Russian FSB Cross Site Scripting

The Russian FSB appears to suffer from a cross site scripting vulnerability. The researchers who discovered it have reported it multiple times to them.

- Link

—

” “Mon, 02 Dec 2024

Laravel 11.0 Cross Site Scripting

Laravel version 11.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 02 Dec 2024

Nvidia GeForce 11.0.1.163 Unquoted Service Path

Nvidia GeForce version 11.0.1.163 suffers from an unquoted service path vulnerability.

- Link

—

” “Mon, 02 Dec 2024

Intelligent Security System SecurOS Enterprise 11 Unquoted Service Path

Intelligent Security System SecurOS Enterprise version 11 suffers from an unquoted service path vulnerability.

- Link

—

” “Wed, 27 Nov 2024

ABB Cylon Aspect 3.08.01 vstatConfigurationDownload.php Configuration Download

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated configuration download vulnerability. This can be exploited to download the CSV DB that contains the configuration mappings information via the VMobileImportExportServlet by directly calling the vstatConfigurationDownload.php script.

- Link

—

” “Wed, 27 Nov 2024

Akuvox Smart Intercom/Doorphone ServicesHTTPAPI Improper Access Control

The Akuvox Smart Intercom/Doorphone suffers from an insecure service API access control. The vulnerability in ServicesHTTPAPI endpoint allows users with ”User” privileges to modify API access

settings and configurations. This improper access control permits privilege escalation, enabling unauthorized access to administrative functionalities. Exploitation of this issue could compromise system integrity and lead to unauthorized system modifications.

- Link

—

” “Fri, 22 Nov 2024

CUPS IPP Attributes LAN Remote Code Execution

This Metasploit module exploits vulnerabilities in OpenPrinting CUPS, which is running by default on most Linux distributions. The vulnerabilities allow an attacker on the LAN to advertise a malicious printer that triggers remote code execution when a victim sends a print job to the malicious printer. Successful exploitation requires user interaction, but no CUPS services need to be reachable via accessible ports. Code execution occurs in the context of the lp user. Affected versions are cups-browsed less than or equal to 2.0.1, libcupsfilters versions 2.1b1 and below, libppd versions 2.1b1 and below, and cups-filters versions 2.0.1 and below.

- Link

—

” “Fri, 22 Nov 2024

ProjectSend R1605 Unauthenticated Remote Code Execution

This Metasploit module exploits an improper authorization vulnerability in ProjectSend versions r1295 through r1605. The vulnerability allows an unauthenticated attacker to obtain remote code execution by enabling user registration, disabling the whitelist of allowed file extensions, and uploading a malicious PHP file to the server.

- Link

—

” “Fri, 22 Nov 2024

needrestart Local Privilege Escalation

Qualys discovered that needrestart suffers from multiple local privilege escalation vulnerabilities that allow for root access from an unprivileged user.

- Link

—

” “Fri, 22 Nov 2024

fronsetia 1.1 Cross Site Scripting

fronsetia version 1.1 suffers from a cross site scripting vulnerability.

- Link

—

” “Fri, 22 Nov 2024

fronsetia 1.1 XML Injection

fronsetia version 1.1 suffers from an XML external entity injection vulnerability.

- Link

—

” “Fri, 22 Nov 2024

PowerVR psProcessHandleBase Reuse

PowerVR has an issue where PVRSRVAcquireProcessHandleBase() can cause psProcessHandleBase reuse when PIDs are reused.

- Link

—

” “Fri, 22 Nov 2024

Linux 6.6 Race Condition

A security-relevant race between mremap() and THP code has been discovered. Reaching the buggy code typically requires the ability to create unprivileged namespaces. The bug leads to installing physical address 0 as a page table, which is likely exploitable in several ways: For example, triggering the bug in multiple processes can probably lead to unintended page table sharing, which probably can lead to stale TLB entries pointing to freed pages.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Wed, 11 Dec 2024

ZDI-24-1681: Tungsten Automation Power PDF JPF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1680: Tungsten Automation Power PDF JP2 File Parsing Use-After-Free Information Disclosure Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1679: Tungsten Automation Power PDF JP2 File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1678: Tungsten Automation Power PDF JP2 File Parsing Out-Of-Bounds Read Information

Disclosure Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1677: Tungsten Automation Power PDF JP2 File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1676: ManageEngine Analytics Plus getOAToken Exposed Dangerous Method Privilege Escalation Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1675: AutomationDirect C-More EA9 EAP9 File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1674: AutomationDirect C-More EA9 EAP9 File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1673: AutomationDirect C-More EA9 EAP9 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1672: GFI Archiver Store Service Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1671: GFI Archiver Telerik Web UI Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1670: GFI Archiver Core Service Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1669: Veritas Enterprise Vault MonitoringMiddleTier Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1668: Veritas Enterprise Vault Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1667: Veritas Enterprise Vault Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1666: Veritas Enterprise Vault Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1665: Veritas Enterprise Vault Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1664: Veritas Enterprise Vault Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1663: Veritas Enterprise Vault Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1662: Veritas Enterprise Vault MobileHTMLView Cross-Site Scripting Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1661: Veritas Enterprise Vault HTMLView Cross-Site Scripting Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1660: Veritas Enterprise Vault HTMLView Cross-Site Scripting Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1659: Veritas Enterprise Vault HTMLView Cross-Site Scripting Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1658: Microsoft Edge File Extension Spoofing Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1657: Microsoft Windows Directory Traversal Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1656: Delta Electronics CNCSoft-G2 DPAX File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Dec 2024

ZDI-24-1655: Rockwell Automation Arena Simulation DOE File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Dec 2024

ZDI-24-1654: Rockwell Automation Arena Simulation DOE File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Dec 2024

ZDI-24-1653: Rockwell Automation Arena Simulation DOE File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Dec 2024

ZDI-24-1652: Rockwell Automation Arena Simulation DOE File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Dec 2024

ZDI-24-1651: Rockwell Automation Arena Simulation DOE File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Dec 2024

ZDI-24-1650: Rockwell Automation Arena Simulation DOE File Parsing Use of Uninitialized Variable Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Dec 2024

ZDI-24-1649: Rockwell Automation Arena Simulation DOE File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Dec 2024

ZDI-24-1648: Linux Kernel Bluetooth HCI Request Race Condition Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 10 Dec 2024

ZDI-24-1647: BlueZ Classic HID Missing Authentication Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Dec 2024

ZDI-24-1486: G DATA Total Security Incorrect Permission Assignment Local Privilege Escalation Vul-

nerability

- Link

—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Gehackt via Nachbar... oder die Palo Alto.

Zum Youtube Video

6 Cyberangriffe: (Dez)

Datum	Opfer	Land	Information
2024-12-09	Muswellbrook Shire Council	[AUS]	Link
2024-12-09	Wood County	[USA]	Link
2024-12-08	Societatea Energetica Electrica S.A.	[GBR]	Link
2024-12-08	Fundación Arturo López Pérez (FALP)	[CHL]	Link
2024-12-07	Vidymed	[CHE]	Link
2024-12-04	Fournisseur de services responsable de la collecte des amendes en retard au Manitoba	[CAN]	Link
2024-12-02	Pembina Trails School Division	[CAN]	Link
2024-12-02	Wayne-Westland Community Schools	[USA]	Link
2024-12-02	ITO EN (North America) INC.	[USA]	Link
2024-12-01	PIH Health	[USA]	Link
2024-12-01	Klinikum Ingolstadt	[DEU]	Link

7 Ransomware-Erpressungen: (Dez)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-12-12	[Brasilmad]	sarcoma	Link
2024-12-11	[cityofmarlow.com]	safepay	Link
2024-12-11	[nbkenney.com]	safepay	Link
2024-12-05	[Watsonville Community Hospital]	termite	Link
2024-12-11	[Locke Solutions , LLC]	nitrogen	Link
2024-12-11	[CW Lighting, LLC]	nitrogen	Link
2024-12-11	[Compass Communications]	raworld	Link
2024-12-11	[Interforos Casting]	killsec	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-12-11	[Sarah Car Care]	everest	Link
2024-12-11	[Primary Plus]	qilin	Link
2024-12-11	[AC Technical Systems]	qilin	Link
2024-12-11	[Bianco Brain & Spine]	qilin	Link
2024-12-11	[Tejas Office Products, Inc.]	nitrogen	Link
2024-12-11	[quiztarget.com]	funksec	Link
2024-12-11	[Planters Telephone Cooperative (planters.net)]	fog	Link
2024-12-11	[www.minerasancristobal.com]	apt73	Link
2024-12-02	[Westerstrand Urfabrik AB]	bluebox	Link
2024-12-03	[PH ARCHITECTURE]	bluebox	Link
2024-12-11	[Matagrano]	akira	Link
2024-12-11	[Renée Blanche]	akira	Link
2024-12-11	[Nova Pole International Inc.]	akira	Link
2024-12-11	[Rutherford County Schools]	rhysida	Link
2024-12-11	[mandiricoal.net]	funksec	Link
2024-12-11	[dealplexus.com]	funksec	Link
2024-12-10	[Inmobiliaria Armas]	medusa	Link
2024-12-10	[Bergerhof]	medusa	Link
2024-12-10	[Ainsworth Game Technology Limited]	medusa	Link
2024-12-10	[Hydra-Matic Packing]	lynx	Link
2024-12-10	[singularanalysts.com]	funksec	Link
2024-12-10	[gervetusa.com]	funksec	Link
2024-12-10	[fpsc-anz.com]	funksec	Link
2024-12-10	[Orthopaedie-hof.de]	cloak	Link
2024-12-10	[Ukh-hof.de]	cloak	Link
2024-12-10	[www.appicgarage.com]	funksec	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-12-10	[wacer.com.au]	funksec	Link
2024-12-10	[thebetareview.com]	funksec	Link
2024-12-10	[senseis.xmp.net]	funksec	Link
2024-12-10	[fpsc-anz.com Breach]	funksec	Link
2024-12-10	[tectaamerica.com]	ransomhub	Link
2024-12-10	[Mission Constructors , Inc.]	nitrogen	Link
2024-12-10	[Haji Husein Alireza]	incransom	Link
2024-12-10	[Telecom Namibia]	hunters	Link
2024-12-10	[kurosu.com.py]	funksec	Link
2024-12-10	[workers.com.zm]	funksec	Link
2024-12-10	[leadboxhq.com]	apt73	Link
2024-12-10	[Matandy (matandy.com)]	akira	Link
2024-12-10	[workers.com.zm Breach]	funksec	Link
2024-12-10	[Corporación BJR]	akira	Link
2024-12-10	[Global Insurance Agency LLC]	bianlian	Link
2024-12-10	[Conrey Insurance Brokers & Risk Managers]	akira	Link
2024-12-10	[Aruba Productions]	akira	Link
2024-12-10	[Lakeside Sod Supply]	akira	Link
2024-12-09	[Proyectos y Seguros]	akira	Link
2024-12-10	[womenscare.com]	ransomhub	Link
2024-12-10	[greenscape.us.com]	ransomhub	Link
2024-12-10	[Physicians' Primary Care of Southwest Florida]	bianlian	Link
2024-12-10	[nedamaritime.gr]	blackout	Link
2024-12-03	[Equity & Advisory]	lynx	Link
2024-12-10	[kurosu.com.py Breach]	funksec	Link
2024-12-09	[gervetusa.com Breach]	funksec	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-12-09	[singularanalysts.com Breach]	funksec	Link
2024-12-04	[www.lasalleinc.com]	ransomhub	Link
2024-12-09	[inia.es]	ransomhub	Link
2024-12-09	[precisediagnosticspacs warn]	funksec	Link
2024-12-09	[melhorcompraclube.com.br]	apt73	Link
2024-12-09	[Hosting.co.uk]	lynx	Link
2024-12-09	[sincorpe.org.br]	funksec	Link
2024-12-09	[pti.agency]	funksec	Link
2024-12-09	[www.bms.com]	apt73	Link
2024-12-09	[bankily.mr]	apt73	Link
2024-12-09	[Cipla]	akira	Link
2024-12-09	[Consumers Builders Supply]	akira	Link
2024-12-09	[ECBM]	akira	Link
2024-12-06	[Pelstar]	akira	Link
2024-12-06	[Pb Loader]	akira	Link
2024-12-06	[Jamaica Bearings Group]	akira	Link
2024-12-06	[Weinberg & Schwartz LLC]	akira	Link
2024-12-05	[Milwaukee Cylinder]	akira	Link
2024-12-05	[Davis Immigration Law Office]	akira	Link
2024-12-05	[Séguin Haché SENCRL]	akira	Link
2024-12-04	[Coffee Beanery]	akira	Link
2024-12-04	[C Pathe]	akira	Link
2024-12-09	[Boston Chinatown Neighborhood Center]	interlock	Link
2024-12-08	[Town of Whitestown - NY Highway Department]	qilin	Link
2024-12-08	[spdyn.de technology]	funksec	Link
2024-12-08	[ncfe.org.in]	funksec	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-12-08	[Gulf Petrochemical Services & Trading]	sarcoma	Link
2024-12-07	[uniamarmores]	funksec	Link
2024-12-07	[zero5]	funksec	Link
2024-12-07	[FunkLocker]	funksec	Link
2024-12-07	[Matlock Security Services]	rhysida	Link
2024-12-07	[ayswrewards]	funksec	Link
2024-12-07	[Arc Community Services Inc]	incransom	Link
2024-12-07	[Black Creek Community Health Centre (bcch.local)]	incransom	Link
2024-12-07	[CO-VER Power Technology SpA]	everest	Link
2024-12-06	[T&M Equipment]	kairos	Link
2024-12-06	[RJM Marketing]	interlock	Link
2024-12-06	[Medical Technology Industries, Inc.]	everest	Link
2024-12-05	[Brodsky Renehan Pearlstein & Bouquet, Chartered]	medusa	Link
2024-12-06	[Precision Walls]	dragonforce	Link
2024-12-05	[Levicoff Law Firm, P.C]	medusa	Link
2024-12-06	[mtgazeta.uz]	funksec	Link
2024-12-06	[LTI Trucking Services]	bianlian	Link
2024-12-06	[Blue Yonder]	termite	Link
2024-12-06	[pro-mec.com]	ransomhub	Link
2024-12-06	[Pan Gulf Holding]	sarcoma	Link
2024-12-06	[pez.com]	abyss	Link
2024-12-05	[ctsjo.com]	funksec	Link
2024-12-05	[Standard Calibrations]	play	Link
2024-12-05	[NatAlliance Securities]	play	Link
2024-12-05	[ITO EN]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-12-05	[Max Trans]	play	Link
2024-12-05	[azpay.me]	apt73	Link
2024-12-05	[SRP Federal Credit Union]	nitrogen	Link
2024-12-05	[Anonymous Victim]	sarcoma	Link
2024-12-05	[Dorner (dorner-gmbh.de)]	fog	Link
2024-12-05	[Star Shuttle Inc.]	bianlian	Link
2024-12-05	[hanwhacimarron.com]	ransomhub	Link
2024-12-05	[edizionidottrinari]	funksec	Link
2024-12-05	[altuslab]	funksec	Link
2024-12-04	[frigopesca.com.ec]	ransomhub	Link
2024-12-05	[USA2ME]	killsec	Link
2024-12-05	[www.aliorbank.pl]	apt73	Link
2024-12-04	[Donnewalddistributing]	cloak	Link
2024-12-04	[islandphoto.com]	ransomhub	Link
2024-12-04	[troxlerlabs.com]	ransomhub	Link
2024-12-04	[hobokennj.gov]	threeam	Link
2024-12-04	[NTrust]	raworld	Link
2024-12-04	[copral.com.br]	lockbit3	Link
2024-12-04	[Deloitte UK]	BrainCipher	Link
2024-12-04	[uniaomarmores]	funksec	Link
2024-12-04	[westbankcorp.com]	blackbasta	Link
2024-12-04	[snatt.it]	blackbasta	Link
2024-12-04	[lornestewartgroup.com]	blackbasta	Link
2024-12-04	[vossko.de]	blackbasta	Link
2024-12-04	[www.certifiedinfosec.com]	apt73	Link
2024-12-04	[FF Steel]	sarcoma	Link
2024-12-03	[www.sefiso-atlantique.fr]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-12-03	[marietta-city.org]	ransomhub	Link
2024-12-03	[westbornmarket.com]	ransomhub	Link
2024-12-04	[www.lasalle.com]	ransomhub	Link
2024-12-04	[kingdom]	funksec	Link
2024-12-04	[albazaar]	funksec	Link
2024-12-04	[rscn.org.jo]	funksec	Link
2024-12-04	[verificativa]	funksec	Link
2024-12-04	[intbizth]	funksec	Link
2024-12-04	[xui.one]	funksec	Link
2024-12-04	[x-cart automotive]	funksec	Link
2024-12-04	[IFA Paris]	funksec	Link
2024-12-04	[styched]	funksec	Link
2024-12-04	[Smart-it-partner]	funksec	Link
2024-12-04	[USA Network]	funksec	Link
2024-12-04	[Zero 5]	funksec	Link
2024-12-03	[Marine Stores Guide]	qilin	Link
2024-12-03	[www.giorgiovisconti.it]	ransomhub	Link
2024-12-03	[www.goethe-university-frankfurt.de]	ransomhub	Link
2024-12-03	[www.siapenet.gov.br]	apt73	Link
2024-12-03	[InterCon Construction]	hunters	Link
2024-12-03	[Conteg]	hunters	Link
2024-12-03	[Royce Corporation]	BrainCipher	Link
2024-12-03	[ACM_IT]	argonauts	Link
2024-12-03	[RDC]	argonauts	Link
2024-12-03	[Goodwill North Central Texas]	rhysida	Link
2024-12-03	[Harel Insurance (Shirbit Server)]	handala	Link
2024-12-02	[New Age Micro]	lynx	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-12-02	[Billaud Segeba]	qilin	Link
2024-12-02	[salesgig.com]	darkvault	Link
2024-12-02	[KHKKLOW.com]	ransomhub	Link
2024-12-02	[G-ONE AUTO PARTS DE MÉXICO, S.A. DE C.V.]	BrainCipher	Link
2024-12-02	[Conlin’s Pharmacy (conlinspharmacy.com)]	fog	Link
2024-12-02	[Mmaynewagemicro]	lynx	Link
2024-12-02	[Avico Spice]	medusa	Link
2024-12-02	[Down East Granite]	medusa	Link
2024-12-02	[Wiley Metal Fabricating]	medusa	Link
2024-12-01	[shapesmfg.com]	ransomhub	Link
2024-12-01	[qualitybillingservice.com]	ransomhub	Link
2024-12-01	[tascosaofficemachines.com]	ransomhub	Link
2024-12-01	[costelloeye.com]	ransomhub	Link
2024-12-01	[McKibbin]	incransom	Link
2024-12-01	[Alpine Ear Nose & Throat]	bianlian	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.