Cybersecurity Morgenreport

Ausgabe: 20231123

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

Security-News

Heise - Security-Alert

Mozilla erweitert Datenschutz und Sicherheit von Firefox und Thunderbird
Durch Schwachstellen in Mozillas Mailclient und Webbbrowser kann Schadcode schlüpfen. Außerdem wurde der Datenschutz verbessert.
- Link

—

Sicherheitsforscher finden kritische Fehler in KI-Werkzeugen Ray, MLflow und H2O
Die beliebten Werkzeuge für KI-Anwendungen leiden unter Codeschmuggel, illegitimen Dateimanipulationen und anderen Bugs. Nicht immer sind Updates verfügbar.
- Link

—

Synology schließt kritische Firmware-Lücke in Überwachungskameras
Angreifer können eigenen Code auf Überwachungskameras von Synology ausführen.
- Link

—

Updates für Trellix ePolicy Orchestrator schließen Sicherheitslücken
Trellix, Nachfolger von McAfee und FireEye, hat den ePolicy Orchestrator aktualisiert. Das Update schließt etwa eine hochriskant eingestufte Schwachstelle.
- Link

—

Code-Schmuggel: Neue Splunk-Versionen beheben Sicherheitslücken
Unsichere XML-Verarbeitung und ungenügende Prüfung von Logeinträgen ermöglichten Angreifern, eigenen Code in Splunk-Produkte zu schleusen.
- Link

—

Sicherheitsupdates: Juniper Secure Analytics ist angreifbar
Angreifer können Lücken in Junipers SIEM-Lösung als Sprungbrett ausnutzen und sich zum Root-Nutzer machen.
- Link

—

FortiNet flickt schwere Sicherheitslücken in FortiOS und anderen Produkten
Neben FortiOS und FortiClient sind auch FortiSIEM, FortiWLM und weitere von zum Teil kritischen Security-Fehlern betroffen. Admins sollten patchen.
- Link

—

Bildbearbeitung: Angreifer können Gimp Schadcode unterjubeln
Die freie Open-Source-Bildbearbeitung Gimp ist in Version 2.10.36 erschienen. Sie schließt Sicherheitslücken, die Codeschmuggel erlauben.
- Link

—

WordPress-Plug-in: Lücke in WP Fastest Cache gefährdet hunderttausende Websites
Durch ein Schlupfloch in WP Fastest Cache sind unbefugte Zugriffe auf WordPress-Websites vorstellbar. Ein Sicherheitsupdate schafft Abhilfe.
- Link

—

Patchday: Intel patcht sich durch sein Produktportfolio
Angreifer können mehrere Komponenten von Intel attackieren. In vielen Fällen sind DoS-Attacken möglich.
- Link

—

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.

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.

CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-4966	0.922670000	0.987050000	Link
CVE-2023-46747	0.965530000	0.995000000	Link
CVE-2023-46604	0.966470000	0.995330000	Link
CVE-2023-42793	0.972640000	0.998120000	Link
CVE-2023-38035	0.970400000	0.996930000	Link
CVE-2023-35078	0.964440000	0.994560000	Link
CVE-2023-34362	0.930390000	0.988010000	Link
CVE-2023-34039	0.925730000	0.987480000	Link
CVE-2023-33246	0.970860000	0.997160000	Link
CVE-2023-32315	0.957520000	0.992620000	Link
CVE-2023-30625	0.925770000	0.987490000	Link
CVE-2023-30013	0.925700000	0.987480000	Link
CVE-2023-28771	0.918550000	0.986550000	Link
CVE-2023-27372	0.971190000	0.997310000	Link
CVE-2023-27350	0.971980000	0.997750000	Link
CVE-2023-26469	0.915280000	0.986160000	Link
CVE-2023-26360	0.913940000	0.986020000	Link
CVE-2023-25717	0.962680000	0.993920000	Link
CVE-2023-25194	0.910980000	0.985700000	Link
CVE-2023-2479	0.961880000	0.993680000	Link
CVE-2023-24489	0.969450000	0.996550000	Link
CVE-2023-22518	0.967630000	0.995810000	Link
CVE-2023-22515	0.955290000	0.992100000	Link
CVE-2023-21839	0.958640000	0.992890000	Link
CVE-2023-21823	0.955130000	0.992050000	Link
CVE-2023-21554	0.961220000	0.993510000	Link
CVE-2023-20887	0.950720000	0.991160000	Link
CVE-2023-1671	0.952600000	0.991540000	Link
CVE-2023-0669	0.966380000	0.995300000	Link

BSI - Warn- und Informationsdienst (WID)

Wed, 22 Nov 2023

[UPDATE] [hoch] Red Hat Satellite: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat Satellite ausnutzen, um

beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Wed, 22 Nov 2023
[NEU] [hoch] Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand zu verursachen.
- Link

—

Wed, 22 Nov 2023
[NEU] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen
Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, beliebigen Code auszuführen oder Dateien zu manipulieren.
- Link

—

Wed, 22 Nov 2023
[NEU] [hoch] Atlassian Bamboo, Atlassian Bitbucket, Atlassian Confluence and Atlassian Jira Software: Mehrere Schwachstellen
Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Atlassian Bamboo, Atlassian Bitbucket, Atlassian Confluence und Atlassian Jira Software ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen oder einen Cross-Site-Scripting-Angriff durchzuführen.
- Link

—

Wed, 22 Nov 2023
[NEU] [UNGEPATCHT] [kritisch] D-LINK G416 Router: Mehrere Schwachstellen
Ein entfernter anonymer Angreifer kann mehrere Schwachstellen im D-LINK G416 Routern ausnutzen, um beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.
- Link

—

Wed, 22 Nov 2023
[NEU] [hoch] Red Hat OpenStack: Schwachstelle ermöglicht Erlangung erweiterter Privilegien
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat OpenStack ausnutzen, um erweiterte Privilegien zu erlangen.
- Link

—

Wed, 22 Nov 2023
[UPDATE] [hoch] Microsoft Developer Tools: Mehrere Schwachstellen
Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in verschiedenen Microsoft Developer Tools ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.
- Link

—

Wed, 22 Nov 2023
[NEU] [hoch] ownCloud: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in ownCloud ausnutzen, um Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen und Dateien zu manipulieren.
- Link

—

Wed, 22 Nov 2023
[UPDATE] [hoch] Ruby: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Ruby ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Wed, 22 Nov 2023
[UPDATE] [hoch] Red Enterprise Linux Advanced Virtualization: Mehrere Schwachstellen
Ein entfernter oder lokaler, authentisierter Angreifer kann mehrere Schwachstellen in Red Enterprise Linux Advanced Virtualization ausnutzen, um einen Denial of Service zu verursachen, Sicherheitsvorkehrungen zu

umgehen, beliebigen Code auszuführen und Informationen offenzulegen.
- Link
—
Wed, 22 Nov 2023
[UPDATE] [hoch] Samba: Mehrere Schwachstellen
Ein entfernter, authetisierter oder anonymer Angreifer kann mehrere Schwachstellen in Samba ausnutzen, um Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen, seine Rechte zu erweitern und die Domäne vollständig zu kompromittieren.
- Link
—
Wed, 22 Nov 2023
[UPDATE] [kritisch] Samba: Mehrere Schwachstellen
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Samba ausnutzen, um Informationen offenzulegen, um einen Denial of Service Zustand herbeizuführen, um Rechte zu erlangen und um beliebigen Code mit Root-Rechten auszuführen.
- Link
—
Wed, 22 Nov 2023
[UPDATE] [hoch] Ruby: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Ruby ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service zu verursachen.
- Link
—
Wed, 22 Nov 2023
[UPDATE] [hoch] Python: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Python ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Wed, 22 Nov 2023
[UPDATE] [hoch] GIMP: Schwachstelle ermöglicht Denial of Service
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in GIMP ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link
—
Wed, 22 Nov 2023
[UPDATE] [hoch] Samba: Mehrere Schwachstellen
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Samba ausnutzen, um Sicherheitsvorkehrungen zu umgehen, Informationen offenzulegen, einen Denial of Service Zustand zu verursachen oder seine Rechte zu erweitern.
- Link
—
Wed, 22 Nov 2023
[UPDATE] [hoch] Python: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Python ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Wed, 22 Nov 2023
[UPDATE] [hoch] Ruby: Schwachstelle ermöglicht Manipulation von Dateien
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Ruby ausnutzen, um Dateien zu manipulieren.
- Link
—
Wed, 22 Nov 2023
[UPDATE] [hoch] Samba: Mehrere Schwachstellen ermöglichen Privilegieneskalation
Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Samba ausnutzen, um seine Privilegien zu erhöhen.
- Link
—
Wed, 22 Nov 2023
[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

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

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
11/22/2023	[Foxit PDF Reader < 2023.3 Multiple Vulnerabilities]	critical
11/22/2023	[Foxit PDF Editor < 2023.3 Multiple Vulnerabilities]	critical
11/22/2023	[Slackware Linux 15.0 / current mozilla-thunderbird Multiple Vulnerabilities (SSA:2023-326-01)]	critical
11/22/2023	[Mozilla Firefox ESR < 115.5.0]	critical
11/22/2023	[Mozilla Firefox ESR < 115.5.0]	critical
11/22/2023	[Mozilla Thunderbird < 115.5]	critical
11/22/2023	[Mozilla Thunderbird < 115.5]	critical
11/22/2023	[RHEL 8 : samba (RHSA-2023:7467)]	critical
11/22/2023	[Oracle Linux 8 : dotnet7.0 (ELSA-2023-7256)]	critical
11/22/2023	[Oracle Linux 8 : nodejs:20 (ELSA-2023-7205)]	critical
11/22/2023	[Debian DSA-5561-1 : firefox-esr - security update]	critical
11/22/2023	[SUSE SLES15 / openSUSE 15 Security Update : apache2-mod_jk (SUSE-SU-2023:4513-1)]	high
11/22/2023	[SUSE SLES15 Security Update : ucode-intel (SUSE-SU-2023:4510-1)]	high
11/22/2023	[SUSE SLES15 Security Update : util-linux (SUSE-SU-2023:4512-1)]	high
11/22/2023	[SUSE SLES15 Security Update : strongswan (SUSE-SU-2023:4516-1)]	high
11/22/2023	[SUSE SLES15 Security Update : strongswan (SUSE-SU-2023:4515-1)]	high
11/22/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : strongswan (SUSE-SU-2023:4514-1)]	high
11/22/2023	[Tenable Security Center 5.23.1 / 6.0.0 / 6.1.0 / 6.1.1 / 6.2.0 Multiple Vulnerabilities (TNS-2023-42)]	high
11/22/2023	[Atlassian Confluence 7.13.x / 7.19.x < 7.19.16 (CONFSERVER-93178)]	high
11/22/2023	[Atlassian Confluence 7.13.x / 8.1.x / 8.2.x / 8.3.x / 8.6.0 < 8.6.1 (CONFSERVER-93169)]	high
11/22/2023	[Citrix ADC and Citrix NetScaler Gateway Information Disclosure (CTX579459) (Direct Check)]	high
11/22/2023	[Atlassian Confluence 7.13.x / 7.19.x < 7.19.16 (CONFSERVER-93179)]	high
11/22/2023	[Oracle Linux 7 : Unbreakable Enterprise kernel-container (ELSA-2023-13001)]	high
11/22/2023	[Oracle Linux 8 : Unbreakable Enterprise kernel-container (ELSA-2023-13005)]	high
11/22/2023	[Oracle Linux 8 : open-vm-tools (ELSA-2023-7265)]	high
11/22/2023	[Oracle Linux 7 : kernel (ELSA-2023-7423)]	high
11/22/2023	[Oracle Linux 7 : tigervnc (ELSA-2023-7428)]	high
11/22/2023	[Ubuntu 22.04 LTS / 23.04 / 23.10 : GlusterFS vulnerability (USN-6507-1)]	high
11/22/2023	[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Apache HTTP Server vulnerabilities (USN-6506-1)]	high
11/22/2023	[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : nghttp2 vulnerability (USN-6505-1)]	high

Datum	Schwachstelle	Bewertung
11/22/2023	[Ubuntu 22.04 LTS / 23.04 / 23.10 : tracker-miners vulnerability (USN-6504-1)]	high
11/22/2023	[RHEL 9 : squid (RHSA-2023:7465)]	high
11/22/2023	[FreeBSD : electron{25,26} – use after free in Garbage Collection (147353a3-c33b-46d1-b751-e72c0d7f29df)]	high
11/22/2023	[Fedora 37 : microcode_ctl (2023-40e71fe5b9)]	high
11/22/2023	[Fedora 39 : openvpn (2023-d9d55a0bfc)]	high
11/22/2023	[Fedora 39 : chromium (2023-9425bb0115)]	high
11/22/2023	[Debian DLA-3660-1 : gnutls28 - LTS security update]	high
11/22/2023	[Debian DSA-5562-1 : tor - security update]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits der letzten 5 Tage

“Wed, 22 Nov 2023
WordPress UserPro 5.1.x Password Reset / Authentication Bypass / Escalation
WordPress UserPro plugin versions 5.1.1 and below suffer from an insecure password reset mechanism, information disclosure, and authentication bypass vulnerabilities. Versions 5.1.4 and below suffer from privilege escalation and shortcode execution vulnerabilities.
- Link
—
” “Mon, 20 Nov 2023
Magento 2.4.6 XSLT Server Side Injection
Magento version 2.4.6 XSLT server-side injection proof of concept exploit.
- Link
—
” “Mon, 20 Nov 2023
PHPJabbers Availability Booking Calendar 5.0 Cross Site Scripting
PHPJabbers Availability Booking Calendar version 5.0 suffers from multiple cross site scripting vulnerabilities.
- Link
—
” “Mon, 20 Nov 2023
PHPJabbers Availability Booking Calendar 5.0 CSV Injection
PHPJabbers Availability Booking Calendar version 5.0 suffers from a CSV injection vulnerability.
- Link
—
” “Mon, 20 Nov 2023
GaatiTrack Courier Management System 1.0 Cross Site Scripting
GaatiTrack Courier Management System version 1.0 suffers from multiple cross site scripting vulnerabilities.
- Link
—
” “Mon, 20 Nov 2023
Jorani Leave Management System 1.0.2 Host Header Injection
Jorani Leave Management System version 1.0.2 suffers from a host header injection vulnerability.
- Link
—
” “Mon, 20 Nov 2023
FireBear Improved Import And Export 3.8.6 XSLT Server Side Injection
FireBear Improved Import and Export version 3.8.6 for Magento 2.4.6 suffers from an XSLT server-side injection vulnerability that allows for command execution.
- Link
—
” “Mon, 20 Nov 2023
Shuttle Booking Software 2.0 Cross Site Scripting
Shuttle Booking Software version 2.0 suffers from multiple persistent cross site scripting vulnerabilities.
- Link
—
” “Fri, 17 Nov 2023
Magento 2.4.6 XSLT Server Side Injection / Command Execution
Magento version 2.4.6 suffers from an XSLT server side injection vulnerability that allows for remote command execution.
- Link
—
” “Wed, 15 Nov 2023
EzViz Studio 2.2.0 DLL Hijacking
EzViz Studio version 2.2.0 suffers from a dll hijacking vulnerability.
- Link
—
” “Tue, 14 Nov 2023
EnBw SENEC Legacy Storage Box Log Disclosure
EnBw SENEC Legacy Storage Box versions 1 through 3 suffer from a log disclosure vulnerability.

- Link

—

” “Tue, 14 Nov 2023

AjaxPro Deserialization Remote Code Execution

This Metasploit module leverages an insecure deserialization of data to get remote code execution on the target OS in the context of the user running the website which utilized AjaxPro. To achieve code execution, the module will construct some JSON data which will be sent to the target. This data will be deserialized by the AjaxPro JsonDeserializer and will trigger the execution of the payload. All AjaxPro versions prior to 21.10.30.1 are vulnerable to this issue, and a vulnerable method which can be used to trigger the deserialization exists in the default AjaxPro namespace. AjaxPro 21.10.30.1 removed the vulnerable method, but if a custom method that accepts a parameter of type that is assignable from ObjectDataProvider (e.g. object) exists, the vulnerability can still be exploited. This module has been tested successfully against official AjaxPro on version 7.7.31.1 without any modification, and on version 21.10.30.1 with a custom vulnerable method added.

- Link

—

” “Tue, 14 Nov 2023

Apache ActiveMQ Unauthenticated Remote Code Execution

This Metasploit module exploits a deserialization vulnerability in the OpenWire transport unmarshaller in Apache ActiveMQ. Affected versions include 5.18.0 through to 5.18.2, 5.17.0 through to 5.17.5, 5.16.0 through to 5.16.6, and all versions before 5.15.16.

- Link

—

” “Tue, 14 Nov 2023

ZoneMinder Snapshots Command Injection

This Metasploit module exploits an unauthenticated command injection in zoneminder that can be exploited by appending a command to an action of the snapshot view. Versions prior to 1.36.33 and 1.37.33 are affected.

- Link

—

” “Tue, 14 Nov 2023

Cisco IOX XE Unauthenticated Remote Code Execution

This Metasploit module leverages both CVE-2023-20198 and CVE-2023-20273 against vulnerable instances of Cisco IOS XE devices which have the web UI exposed. An attacker can execute a payload with root privileges. The vulnerable IOS XE versions are 16.1.1, 16.1.2, 16.1.3, 16.2.1, 16.2.2, 16.3.1, 16.3.2, 16.3.3, 16.3.1a, 16.3.4, 16.3.5, 16.3.5b, 16.3.6, 16.3.7, 16.3.8, 16.3.9, 16.3.10, 16.3.11, 16.4.1, 16.4.2, 16.4.3, 16.5.1, 16.5.1a, 16.5.1b, 16.5.2, 16.5.3, 16.6.1, 16.6.2, 16.6.3, 16.6.4, 16.6.5, 16.6.4s, 16.6.4a, 16.6.5a, 16.6.6, 16.6.5b, 16.6.7, 16.6.7a, 16.6.8, 16.6.9, 16.6.10, 16.7.1, 16.7.1a, 16.7.1b, 16.7.2, 16.7.3, 16.7.4, 16.8.1, 16.8.1a, 16.8.1b, 16.8.1s, 16.8.1c, 16.8.1d, 16.8.2, 16.8.1e, 16.8.3, 16.9.1, 16.9.2, 16.9.1a, 16.9.1b, 16.9.1s, 16.9.1c, 16.9.1d, 16.9.3, 16.9.2a, 16.9.2s, 16.9.3h, 16.9.4, 16.9.3s, 16.9.3a, 16.9.4c, 16.9.5, 16.9.5f, 16.9.6, 16.9.7, 16.9.8, 16.9.8a, 16.9.8b, 16.9.8c, 16.10.1, 16.10.1a, 16.10.1b, 16.10.1s, 16.10.1c, 16.10.1e, 16.10.1d, 16.10.2, 16.10.1f, 16.10.1g, 16.10.3, 16.11.1, 16.11.1a, 16.11.1b, 16.11.2, 16.11.1s, 16.11.1c, 16.12.1, 16.12.1s, 16.12.1a, 16.12.1c, 16.12.1w, 16.12.2, 16.12.1y, 16.12.2a, 16.12.3, 16.12.8, 16.12.2s, 16.12.1x, 16.12.1t, 16.12.2t, 16.12.4, 16.12.3s, 16.12.1z, 16.12.3a, 16.12.4a, 16.12.5, 16.12.6, 16.12.1z1, 16.12.5a, 16.12.5b, 16.12.1z2, 16.12.6a, 16.12.7, 16.12.9, 16.12.10, 17.1.1, 17.1.1a, 17.1.1s, 17.1.2, 17.1.1t, 17.1.3, 17.2.1, 17.2.1r, 17.2.1a, 17.2.1v, 17.2.2, 17.2.3, 17.3.1, 17.3.2, 17.3.3, 17.3.1a, 17.3.1w, 17.3.2a, 17.3.1x, 17.3.1z, 17.3.3a, 17.3.4, 17.3.5, 17.3.4a, 17.3.6, 17.3.4b, 17.3.4c, 17.3.5a, 17.3.5b, 17.3.7, 17.3.8, 17.4.1, 17.4.2, 17.4.1a, 17.4.1b, 17.4.1c, 17.4.2a, 17.5.1, 17.5.1a, 17.5.1b, 17.5.1c, 17.6.1, 17.6.2, 17.6.1w, 17.6.1a, 17.6.1x, 17.6.3, 17.6.1y, 17.6.1z, 17.6.3a, 17.6.4, 17.6.1z1, 17.6.5, 17.6.6, 17.7.1, 17.7.1a, 17.7.1b, 17.7.2, 17.10.1, 17.10.1a, 17.10.1b, 17.8.1, 17.8.1a, 17.9.1, 17.9.1w, 17.9.2, 17.9.1a, 17.9.1x, 17.9.1y, 17.9.3, 17.9.2a, 17.9.1x1, 17.9.3a, 17.9.4, 17.9.1y1, 17.11.1, 17.11.1a, 17.12.1, 17.12.1a, and 17.11.99SW.

- Link

—

” “Tue, 14 Nov 2023

F5 BIG-IP TMUI AJP Smuggling Remote Command Execution

This Metasploit module exploits a flaw in F5’s BIG-IP Traffic Management User Interface (TMU) that enables an external, unauthenticated attacker to create an administrative user. Once the user is created, the module uses the new account to execute a command payload. Both the exploit and check methods automatically delete any temporary accounts that are created.

- Link

—

” “Tue, 14 Nov 2023

MagnusBilling Remote Command Execution

This Metasploit module exploits a command injection vulnerability in MagnusBilling application versions 6.x

and 7.x that allows remote attackers to run arbitrary commands via an unauthenticated HTTP request. A piece of demonstration code is present in lib/icepay/icepay.php, with a call to an exec(). The parameter to exec() includes the GET parameter democ, which is controlled by the user and not properly sanitised/escaped. After successful exploitation, an unauthenticated user is able to execute arbitrary OS commands. The commands run with the privileges of the web server process, typically www-data or asterisk. At a minimum, this allows an attacker to compromise the billing system and its database.
- Link
—
” “Tue, 14 Nov 2023
F5 BIG-IP TMUI Directory Traversal / File Upload / Code Execution
This Metasploit module exploits a directory traversal in F5's BIG-IP Traffic Management User Interface (TMUI) to upload a shell script and execute it as the Unix root user. Unix shell access is obtained by escaping the restricted Traffic Management Shell (TMSH). The escape may not be reliable, and you may have to run the exploit multiple times. Versions 11.6.1-11.6.5, 12.1.0-12.1.5, 13.1.0-13.1.3, 14.1.0-14.1.2, 15.0.0, and 15.1.0 are known to be vulnerable. Fixes were introduced in 11.6.5.2, 12.1.5.2, 13.1.3.4, 14.1.2.6, and 15.1.0.4. Tested against the VMware OVA release of 14.1.2.
- Link
—
” “Tue, 14 Nov 2023
mtk-jpeg Driver Out-Of-Bounds Read / Write
An out-of-bounds read / write due to missing bounds check in the mtk-jpeg driver can lead to memory corruption and potential escalation of privileges.
- Link
—
” “Tue, 14 Nov 2023
Android mtk_jpeg Driver Race Condition / Privilege Escalation
A race condition in the Android mtk_jpeg driver can lead to memory corruption and potential local privilege escalation.
- Link
—
” “Mon, 13 Nov 2023
Maxima Max Pro Power 1.0 486A BLE Traffic Replay
Maxima Max Pro Power with firmware version 1.0 486A suffers from a BLE traffic replay vulnerability that allows for arbitrary unauthorized actions.
- Link
—
” “Mon, 13 Nov 2023
Windows Kernel Containerized Registry Escape
The Microsoft Windows kernel suffers from a containerized registry escape through integer overflows in VrpBuildKeyPath and other weaknesses.
- Link
—
” “Mon, 13 Nov 2023
WordPress Contact Form To Any API 1.1.2 SQL Injection
WordPress Contact Form to Any API plugin version 1.1.2 suffers from a remote SQL injection vulnerability.
- Link
—
” “Mon, 13 Nov 2023
Penglead 2.0 SQL Injection
Penglead version 2.0 suffers from a remote SQL Injection vulnerability that allows for authentication bypass.
- Link
—
” “Mon, 13 Nov 2023
LOYTEC Electronics Insecure Transit / Insecure Permissions / Unauthenticated Access
Products from LOYTEC electronics such as Loytec LWEB-802, L-INX Automation Servers, L-IOB I/O Controllers, and L-VIS Touch Panels suffer from improper access control and insecure transit vulnerabilities.
- Link
—
”

0-Days der letzten 5 Tage

“Wed, 22 Nov 2023
ZDI-23-1719: ManageEngine Recovery Manager Plus getEscapedValue Command Injection Remote Code Execution Vulnerability
- Link
—
” “Mon, 20 Nov 2023
ZDI-23-1718: NETGEAR ProSAFE Network Management System getNodesByTopologyMapSearch SQL Injection Remote Code Execution Vulnerability
- Link
—
” “Mon, 20 Nov 2023
ZDI-23-1717: NETGEAR ProSAFE Network Management System clearAlertByIds SQL Injection Privilege Escalation Vulnerability
- Link
—
”

Die Hacks der Woche

mit Martin Haunschmid

Eine Zeitreise in die Anfänge des hack-for-hire

Zum Youtube Video

Cyberangriffe: (Nov)

Datum	Opfer	Land	Information
2023-11-22	Véligo Location	[FRA]	Link
2023-11-19	Rostocker Straßenbahn AG (RSAG)	[DEU]	Link
2023-11-17	SIAAP (Syndicat Interdépartemental pour l'Assainissement de l'Agglomération Parisienne)	[FRA]	Link
2023-11-17	Mössinger Stadtverwaltung	[DEU]	Link
2023-11-16	Etelä-Savon ammattiopisto Esedu	[FIN]	Link
2023-11-16	Sabre Insurance Group	[GBR]	Link
2023-11-14	Bladen County Government	[USA]	Link
2023-11-14	North Muskegon Public Schools	[USA]	Link
2023-11-14	Beaverton School District	[USA]	Link
2023-11-14	City of Long Beach	[USA]	Link
2023-11-13	Yanfeng	[CHN]	Link
2023-11-13	North Carolina Central University (NCCU)	[USA]	Link
2023-11-12	Huber Heights	[USA]	Link
2023-11-12	Tunstall	[NLD]	Link
2023-11-12	Deutsche Energie-Agentur (Dena)	[DEU]	Link
2023-11-11	Okada Manila	[PHL]	Link
2023-11-10	DP World Australia	[AUS]	Link
2023-11-10	Derichebourg Multiservices	[FRA]	Link
2023-11-10	Glendale Community College (GCC)	[USA]	Link
2023-11-09	Industrial and Commercial Bank of China (ICBC)	[CHN]	Link
2023-11-09	Tri-City Medical Center	[USA]	Link
2023-11-09	Henry County Schools	[USA]	Link
2023-11-08	York Region District School Board	[CAN]	Link
2023-11-08	Hellenic Public Properties Company (ETAD)	[GRC]	Link
2023-11-07	Comhairle nan Eilean Siar	[GBR]	Link
2023-11-07	Harris Center for Mental Health and IDD	[USA]	Link
2023-11-07	Washington State Department of Transportation (WSDOT)	[USA]	Link
2023-11-06	KaDeWe	[DEU]	Link
2023-11-05	Le conseil départemental du Loiret	[FRA]	Link
2023-11-05	Madison Memorial Hospital	[USA]	Link
2023-11-05	Pulaski County Public Schools (PCPS)	[USA]	Link
2023-11-05	Concevis AG	[CHE]	Link
2023-11-04	Butte School District	[USA]	Link
2023-11-02	Infosys McCamish Systems	[USA]	Link
2023-11-02	Crystal Run Healthcare	[USA]	Link
2023-11-01	Mr. Cooper Group	[USA]	Link
2023-11-01	Rekord Fenster Türen	[DEU]	Link
2023-11-01	EDC	[DNK]	Link
2023-11-01	Cogdell Memorial Hospital	[USA]	Link

Ransomware-Erpressungen: (Nov)

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-11-22	[McHale Landscape Design]	play	Link
2023-11-22	[Fidelity National Financial]	alphv	Link
2023-11-22	[Alspec]	akira	Link
2023-11-22	[Custom Engineering &Fabrication, Inc.]	akira	Link
2023-11-22	[IQ Supply Solutions]	akira	Link
2023-11-22	[NESPOLI GROUP]	alphv	Link
2023-11-22	[Community Hospital]	medusa	Link
2023-11-22	[merz-elektro.de]	lockbit3	Link
2023-11-22	[art-eco.it]	lockbit3	Link
2023-11-22	[therobisongroup.com]	lockbit3	Link
2023-11-22	[ds-granit.fr]	threeam	Link
2023-11-21	[APVL ingénierie]	8base	Link
2023-11-21	[Cold Car Spa]	8base	Link
2023-11-21	[La Contabile Spa]	8base	Link
2023-11-21	[DMC Luxembourg]	8base	Link
2023-11-22	[Hills Legal Group Ltd]	8base	Link
2023-11-22	[Brown's Bay Packing Company]	8base	Link
2023-11-22	[Hahn and Clay, Inc.]	8base	Link
2023-11-22	[Imperiali AG]	8base	Link
2023-11-21	[[DATA] Bakrie Group & Bakrie Sumatera Plantations]	alphv	Link
2023-11-21	[floydskerenlaw.com]	lockbit3	Link
2023-11-21	[bnpmedia.com]	lockbit3	Link
2023-11-21	[Verhelst]	cactus	Link
2023-11-21	[Petersen Health Care]	cactus	Link
2023-11-21	[Paul Stuart]	cactus	Link
2023-11-21	[Crystal Lake Health Center]	hunters	Link
2023-11-21	[qautomotive.com.au]	lockbit3	Link
2023-11-21	[martinique.no]	lockbit3	Link
2023-11-21	[phihydraulics.com]	lockbit3	Link
2023-11-21	[St Edmund's College & Prep School]	rhysida	Link
2023-11-21	[helifrusa.com]	lockbit3	Link
2023-11-21	[Bolidt]	bianlian	Link
2023-11-21	[Growers Express]	bianlian	Link
2023-11-21	[NSEIT Limited (a subsidiary of the National Stock Exchange of India)]	bianlian	Link
2023-11-11	[Rc Moore Inc]	noescape	Link
2023-11-10	[Enware Australia Pty Ltd]	noescape	Link
2023-11-20	[sabre.co.uk]	lockbit3	Link
2023-11-20	[nybravestfcu.org]	lockbit3	Link
2023-11-20	[Hampton Newport News CSB]	alphv	Link
2023-11-20	[jlgmarine.com]	blackbasta	Link
2023-11-12	[Studio D.EL.LA. SRL]	knight	Link
2023-11-14	[Barnett Millworks]	knight	Link
2023-11-20	[Dreyfuss Williams & Associates Co., LPA]	knight	Link
2023-11-20	[onyourmark.org]	lockbit3	Link
2023-11-20	[agrovi.dk]	blackbasta	Link
2023-11-20	[arenaproducts.com]	blackbasta	Link
2023-11-20	[etude-villa.fr]	blackbasta	Link
2023-11-16	[UPDATE! FEAM Maintenance]	alphv	Link
2023-11-20	[brownintegratedlogistics.com]	lockbit3	Link
2023-11-20	[British Library]	rhysida	Link
2023-11-22	[Hahn & Clay, Inc.]	8base	Link
2023-11-19	[Tackle West]	alphv	Link
2023-11-19	[U.L. COLEMAN COMPANIES]	alphv	Link
2023-11-19	[Autonomous Flight - @autonomousfly]	alphv	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-11-18	[The DMC]	play	Link
2023-11-18	[nealbrothers.co.uk]	threeam	Link
2023-11-18	[generalrefrig.com]	lockbit3	Link
2023-11-17	[PruittHealth]	noescape	Link
2023-11-17	[ajcfood.com]	lockbit3	Link
2023-11-17	[CENTRE D'AUTO P.R.N. SALABERRY IN]	medusa	Link
2023-11-17	[McCray & Withrow]	medusa	Link
2023-11-17	[Metro MPLS]	akira	Link
2023-11-17	[HAESUNG DS CO Ltd]	qilin	Link
2023-11-05	[Kwik Industries, Inc.]	noescape	Link
2023-11-17	[WellLife Network Inc.]	incransom	Link
2023-11-17	[ATC SA]	akira	Link
2023-11-17	[Select Education Group]	blacksuit	Link
2023-11-17	[edc.dk]	blackbasta	Link
2023-11-17	[villanuevadelaserena.es]	lockbit3	Link
2023-11-17	[Admilla ELAP]	ransomexx	Link
2023-11-17	[Aceromex]	ragroup	Link
2023-11-17	[Chung Hwa Chemical Industrial Works]	ragroup	Link
2023-11-17	[SUMMIT VETERINARY PHARMACEUTICALS LIMITED]	ragroup	Link
2023-11-17	[Informist Media]	ragroup	Link
2023-11-17	[Epstein Law]	qilin	Link
2023-11-16	[Toyota Financial]	medusa	Link
2023-11-17	[owensgroup.uk]	lockbit3	Link
2023-11-17	[hsksgreenhalgh.co.uk]	lockbit3	Link
2023-11-17	[krblaw.com]	lockbit3	Link
2023-11-17	[communitydentalme.org]	lockbit3	Link
2023-11-17	[chicagotrading.com]	lockbit3	Link
2023-11-17	[adyne.com]	lockbit3	Link
2023-11-17	[goodhopeholdings.com]	lockbit3	Link
2023-11-17	[planethomelending.com]	lockbit3	Link
2023-11-15	[Decatur Independent School District]	incransom	Link
2023-11-16	[Consilium staffing llc]	incransom	Link
2023-11-15	[Yamaha Motor Philippines,Inc.]	incransom	Link
2023-11-15	[Guardian Alarm]	incransom	Link
2023-11-15	[SCOLARI Srl]	incransom	Link
2023-11-16	[uchlogistics.co.uk]	blackbasta	Link
2023-11-16	[citycontainer.dk]	blackbasta	Link
2023-11-16	[FEAM Maintenance]	alphv	Link
2023-11-16	[thewalkerschool]	alphv	Link
2023-11-15	[MeridianLink fails to file with the SEC..so we do it for them + 24 hours to pay]	alphv	Link
2023-11-15	[EOS]	lorenz	Link
2023-11-15	[THK Co., Ltd.]	hunters	Link
2023-11-15	[Cardinal MetalWorks]	alphv	Link
2023-11-15	[ADH Health Products Inc]	alphv	Link
2023-11-08	[Ingeniería FULCRUM]	8base	Link
2023-11-09	[Scheidt GmbH]	8base	Link
2023-11-15	[Gallagher Tire, Inc.]	8base	Link
2023-11-15	[MODERNGRAB, S.A.]	8base	Link
2023-11-15	[Storey Trucking Company, Inc.]	8base	Link
2023-11-15	[APREVYA]	8base	Link
2023-11-15	[Lanificio Luigi Colombo S.p.A.]	8base	Link
2023-11-15	[MERRILL Technologies Group]	8base	Link
2023-11-15	[Ontario Pork]	8base	Link
2023-11-15	[Parsons Investments]	8base	Link
2023-11-15	[kwhfreeze.fi]	lockbit3	Link
2023-11-14	[PIKE Technologies]	play	Link
2023-11-14	[Proforma Albrecht]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-11-14	[Fgs]	play	Link
2023-11-14	[Trademark Property]	play	Link
2023-11-14	[Nomot]	play	Link
2023-11-14	[Global Technologies Racing Ltd]	play	Link
2023-11-14	[Thompson Candy]	play	Link
2023-11-14	[Road Scholar Transport]	play	Link
2023-11-14	[KaDeWe]	play	Link
2023-11-14	[Wyatt Detention Center]	play	Link
2023-11-14	[Guntert & Zimmerman]	play	Link
2023-11-14	[ConSpare]	play	Link
2023-11-14	[Premise Health]	alphv	Link
2023-11-15	[MeridianLink]	alphv	Link
2023-11-14	[Gnome Landscapes]	alphv	Link
2023-11-14	[agromatic.de]	blackbasta	Link
2023-11-14	[cmcsheetmetal.com]	blackbasta	Link
2023-11-14	[rekord.de]	blackbasta	Link
2023-11-14	[boulangerieauger.com]	blackbasta	Link
2023-11-14	[maytec.de]	blackbasta	Link
2023-11-14	[SheelaFoam]	alphv	Link
2023-11-14	[Naftor and Grupa Pern (Naftoport/ SIARKOPOL/ SARMATIA/ NAFTOSERWIS) is the most dangerous]	alphv	Link
2023-11-14	[4set.es]	alphv	Link
2023-11-14	[diagnostechs]	cuba	Link
2023-11-14	[Execuzen]	alphv	Link
2023-11-05	[Lander County Convention & Tourism Authority]	noescape	Link
2023-11-10	[Carespring]	noescape	Link
2023-11-13	[shopbentley.com]	blackbasta	Link
2023-11-13	[tarltonandson.com]	lockbit3	Link
2023-11-13	[ASM GLOBAL]	alphv	Link
2023-11-13	[portadelaidefc]	cuba	Link
2023-11-13	[St. Lucie County Tax Collector's]	alphv	Link
2023-11-10	[Bartec Top Holding GmbH]	hunters	Link
2023-11-09	[Garr Silpe, P.C.]	hunters	Link
2023-11-06	[United Africa Group Ltd.]	hunters	Link
2023-11-12	[IDESA group, S.A. De C.V.]	hunters	Link
2023-11-12	[DrilMaco]	hunters	Link
2023-11-03	[Builders Hardware and Hollow Metal, Inc.]	hunters	Link
2023-11-13	[Homeland Inc.]	hunters	Link
2023-11-03	[Deegenbergklinik]	hunters	Link
2023-11-12	[Owens Group]	hunters	Link
2023-11-13	[TCI Co., Ltd.]	hunters	Link
2023-11-03	[Medjet]	hunters	Link
2023-11-13	[United Site Services]	bianlian	Link
2023-11-13	[NSEIT LIMITED]	bianlian	Link
2023-11-13	[Moneris Solutions]	medusa	Link
2023-11-12	[muellersystems.com]	lockbit3	Link
2023-11-13	[msim.de]	lockbit3	Link
2023-11-02	[Putzel Electrical Contractors Inc]	noescape	Link
2023-11-12	[aegean.gr]	lockbit3	Link
2023-11-12	[thewalkerschool.org]	lockbit3	Link
2023-11-12	[modafabrics.com]	lockbit3	Link
2023-11-12	[wombleco.com]	lockbit3	Link
2023-11-12	[cityofclarksville.com]	lockbit3	Link
2023-11-12	[digitaldruck-esser.de]	lockbit3	Link
2023-11-12	[hotelemc2.com]	lockbit3	Link
2023-11-12	[carsonteam.com]	lockbit3	Link
2023-11-12	[plati.it]	lockbit3	Link
2023-11-12	[hotel-ampere-paris.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-11-12	[Pricesmart]	alphv	Link
2023-11-11	[roth-werkzeugbau.de]	lockbit3	Link
2023-11-11	[heinrichseegers.de]	lockbit3	Link
2023-11-11	[aten.com]	lockbit3	Link
2023-11-11	[quifatex.com]	lockbit3	Link
2023-11-11	[vital.co.za]	lockbit3	Link
2023-11-11	[creatz3d.sg]	lockbit3	Link
2023-11-11	[loiret.fr]	lockbit3	Link
2023-11-05	[PAR Group Co]	noescape	Link
2023-11-11	[MHM Health]	rhysida	Link
2023-11-11	[estes-express.com]	lockbit3	Link
2023-11-11	[shawneemilling.com]	abyss	Link
2023-11-11	[motordepot.co.uk]	abyss	Link
2023-11-11	[Dragos Inc]	alphv	Link
2023-11-10	[floortex.com]	lockbit3	Link
2023-11-10	[planning.org]	lockbit3	Link
2023-11-10	[ayakitchens.com]	blackbasta	Link
2023-11-10	[browardfactory.com]	blackbasta	Link
2023-11-10	[boslogistics.eu]	blackbasta	Link
2023-11-10	[morningstarco.com]	lockbit3	Link
2023-11-10	[Mariposa Landscapes, Inc]	alphv	Link
2023-11-10	[Azienda Ospedaliera Universitaria Integrata di Verona]	rhysida	Link
2023-11-10	[aei.cc]	lockbit3	Link
2023-11-09	[Sinotech Group Taiwan]	alphv	Link
2023-11-09	[Rudolf Venture Chemical Inc - Press Release]	monti	Link
2023-11-09	[Magsaysay Maritime - Press Release]	monti	Link
2023-11-09	[SALUS Controls]	akira	Link
2023-11-09	[Battle Motors (CraneCarrier, CCC)]	akira	Link
2023-11-09	[gotocfr.com]	lockbit3	Link
2023-11-09	[City Furniture Hire]	akira	Link
2023-11-09	[Autocommerce]	akira	Link
2023-11-02	[Koh Brothers]	lorenz	Link
2023-11-09	[Cogdell Memorial Hospital]	lorenz	Link
2023-11-09	[Simons Petroleum/Maxum Petroleum/Pilot Thomas Logistics]	akira	Link
2023-11-09	[ggarabia.com]	lockbit3	Link
2023-11-08	[JS Hovnanian & Sons]	play	Link
2023-11-08	[Identification Products]	play	Link
2023-11-08	[M.R. Williams]	play	Link
2023-11-08	[DESIGNA Verkehrsleittechnik]	play	Link
2023-11-08	[The Supply Room Companies & Citron WorkSpaces]	play	Link
2023-11-08	[Ackerman-Estvold]	play	Link
2023-11-08	[Meindl]	play	Link
2023-11-08	[Conditioned Air]	play	Link
2023-11-08	[Inclinator]	play	Link
2023-11-08	[Crown Supply Co]	play	Link
2023-11-08	[fawry.com]	lockbit3	Link
2023-11-08	[amberhillgroup.com]	lockbit3	Link
2023-11-08	[califanocarrelli.it]	blackbasta	Link
2023-11-08	[sheehyware.com]	alphv	Link
2023-11-08	[Michael Garron Hospital]	akira	Link
2023-11-08	[foley.k12.mn.us]	lockbit3	Link
2023-11-08	[gitiusa.com]	lockbit3	Link
2023-11-08	[allenovery.com]	lockbit3	Link
2023-11-08	[NeoDomos]	ciphbit	Link
2023-11-07	[Bakrie Group & Bakrie Sumatera Plantations]	alphv	Link
2023-11-07	[Indah Water Konsortium]	rhysida	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-11-07	[Access to the large database of a US Medical organization]	everest	Link
2023-11-07	[h-tube.com]	blackbasta	Link
2023-11-07	[torrescpa.com]	blackbasta	Link
2023-11-07	[tt-engineering.nl]	blackbasta	Link
2023-11-07	[nicecloud.nl]	blackbasta	Link
2023-11-07	[triflex.nl]	blackbasta	Link
2023-11-07	[cozwolle.nl]	blackbasta	Link
2023-11-07	[Certified Mortgage Planners]	alphv	Link
2023-11-07	[BioPower SustainableEnergy Corporation]	akira	Link
2023-11-07	[BITZER]	akira	Link
2023-11-07	[acawtrustfunds.ca]	blackbasta	Link
2023-11-07	[secci.ca]	blackbasta	Link
2023-11-07	[Hopewell Area School District]	medusa	Link
2023-11-07	[panaya]	cuba	Link
2023-11-07	[prime-art]	cuba	Link
2023-11-07	[ccdrc.pt]	lockbit3	Link
2023-11-07	[Yuxin Automobile Co.Ltd]	ragroup	Link
2023-11-07	[Aceromex (Unpay-Start Leaking)]	ragroup	Link
2023-11-07	[Japan Aviation Electronics Industry, Ltd]	alphv	Link
2023-11-06	[sacksteinlaw.com]	blackbasta	Link
2023-11-06	[good-lawyer.com]	lockbit3	Link
2023-11-06	[EFU Life Assurance]	incransom	Link
2023-11-06	[kbrlaw.com]	lockbit3	Link
2023-11-06	[eyephy.com]	lockbit3	Link
2023-11-06	[Mount St. Mary's Seminary]	rhysida	Link
2023-11-06	[concretevalue.com]	lockbit3	Link
2023-11-06	[howlandlaw.net]	lockbit3	Link
2023-11-06	[GEOCOM]	cactus	Link
2023-11-06	[MultiMasters]	cactus	Link
2023-11-06	[UTI Group]	cactus	Link
2023-11-06	[Comfloresta]	alphv	Link
2023-11-05	[Currax Pharmaceuticals]	alphv	Link
2023-11-05	[Advarra leak]	alphv	Link
2023-11-05	[Weidmann & Associates]	medusa	Link
2023-11-05	[Unimed Blumenau]	medusa	Link
2023-11-05	[Leaguers]	medusa	Link
2023-11-05	[Zon Beachside]	medusa	Link
2023-11-05	[Canadian Psychological Association]	medusa	Link
2023-11-05	[Corsica-Ferries]	alphv	Link
2023-11-05	[penanshin]	alphv	Link
2023-11-05	[lathamcenters.org]	abyss	Link
2023-11-05	[Assurius.be]	qilin	Link
2023-11-05	[unique-relations.at]	qilin	Link
2023-11-05	[SMH Group]	rhysida	Link
2023-11-05	[nckb.com]	lockbit3	Link
2023-11-05	[egco.com]	lockbit3	Link
2023-11-05	[benya.capital]	lockbit3	Link
2023-11-05	[global-value-web.com]	lockbit3	Link
2023-11-05	[aseankorea.org]	lockbit3	Link
2023-11-05	[brlogistics.net]	lockbit3	Link
2023-11-05	[bresselouhannaiseintercom.fr]	lockbit3	Link
2023-11-05	[nfcc.gov.my]	lockbit3	Link
2023-11-05	[sansasecurity.com]	lockbit3	Link
2023-11-05	[emiliacentrale.it]	lockbit3	Link
2023-11-05	[letillet.btprms.com]	lockbit3	Link
2023-11-05	[ospedalecoq.it]	lockbit3	Link
2023-11-05	[springeroil.com]	lockbit3	Link
2023-11-05	[szutest.cz]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-11-05	[mat-antriebstechnik.de]	lockbit3	Link
2023-11-05	[studio483.com]	lockbit3	Link
2023-11-04	[infosysbpm.com]	lockbit3	Link
2023-11-04	[tks.co.th]	lockbit3	Link
2023-11-03	[GeoPoint Surveying]	play	Link
2023-11-03	[APERS]	ciphbit	Link
2023-11-03	[translink.se]	lockbit3	Link
2023-11-03	[tasl.co.th]	lockbit3	Link
2023-11-03	[abhmfg.com]	lockbit3	Link
2023-11-03	[Livability]	incransom	Link
2023-11-03	[portlandtractor.com]	lockbit3	Link
2023-11-03	[unimed.coop.br]	lockbit3	Link
2023-11-03	[jewell.edu]	lockbit3	Link
2023-11-03	[microtrain.net]	lockbit3	Link
2023-11-02	[Warning to Advarra & Gadi!]	alphv	Link
2023-11-01	[Bry-Air]	play	Link
2023-11-02	[JDRM Engineering]	play	Link
2023-11-02	[Craft-Maid]	play	Link
2023-11-02	[Hilyard's]	play	Link
2023-11-02	[North Dakota Grain Inspection Services]	play	Link
2023-11-02	[Gsp Components]	play	Link
2023-11-02	[Ricardo]	play	Link
2023-11-02	[bindagroup.com]	lockbit3	Link
2023-11-02	[lafase.cl]	lockbit3	Link
2023-11-02	[shimano.com]	lockbit3	Link
2023-11-02	[Contact Cottrell and McCullough]	alphv	Link
2023-11-02	[psmicorp.com]	lockbit3	Link
2023-11-02	[imancorp.es]	blackbasta	Link
2023-11-02	[AF Supply]	alphv	Link
2023-11-02	[GO! Handelsschool Aalst]	rhysida	Link
2023-11-01	[Groupe Faubourg]	8base	Link
2023-11-02	[HAL Allergy]	alphv	Link
2023-11-01	[Detroit Symphony Orchestra]	snatch	Link
2023-11-02	[degregoris.com]	lockbit3	Link
2023-11-02	[Bluewater Health (CA) and others]	daixin	Link
2023-11-01	[vitaresearch.com]	lockbit3	Link
2023-11-01	[sanmiguel.iph]	lockbit3	Link
2023-11-01	[steelofcarolina.com]	lockbit3	Link
2023-11-01	[raumberg-gumpenstein.at]	lockbit3	Link
2023-11-01	[kitprofs.com]	lockbit3	Link
2023-11-01	[imprex.es]	lockbit3	Link
2023-11-01	[Hawkeye Area Community Action Program, Inc]	blacksuit	Link
2023-11-01	[Advarra Inc]	alphv	Link
2023-11-01	[summithealth.com]	lockbit3	Link
2023-11-01	[US Claims Solutions]	knight	Link
2023-11-01	[strongtie.com]	blackbasta	Link
2023-11-01	[ampersand.tv]	blackbasta	Link
2023-11-01	[baccarat.com]	blackbasta	Link
2023-11-01	[piemmeonline.it]	blackbasta	Link
2023-11-01	[fortive.com]	blackbasta	Link
2023-11-01	[gannons.co.uk]	blackbasta	Link
2023-11-01	[gsp.com.br]	blackbasta	Link
2023-11-01	[TANATEX Chemicals]	metaencryptor	Link
2023-11-01	[edwardian.com]	blackbasta	Link
2023-11-01	[bionpharma.com]	blackbasta	Link
2023-11-01	[stantonwilliams.com]	blackbasta	Link
2023-11-01	[hugohaeffner.com]	blackbasta	Link
2023-11-01	[intred.it]	blackbasta	Link
2023-11-01	[Town of Lowa]	alphv	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-11-01	[Traxall France]	8base	Link
2023-11-01	[Armstrong Consultants]	8base	Link
2023-11-01	[JAI A/S]	8base	Link
2023-11-01	[Schöler Fördertechnik AG]	8base	Link

Quellen

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

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.