Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241114

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

Sicherheitsupdates: Zoom Room Client & Co. angreifbar

Die Entwickler rüsten verschiedene Zoom-Apps gegen mögliche Angriffe. Davon sind unter anderem macOS und Windows betroffen.

- Link

—

Fortinet stopft Sicherheitslecks in FortiOS, FortiAnalyzer und FortiClient

Sicherheitslücken in FortiClient für Windows, FortiAnalyzer und FortiOS machen die Systeme anfällig für Angriffe. Updates stehen bereit.

- Link

—

Ivanti patcht Endpoint Manager, Avalanche, VPN- und NAC-Software

Ivanti bessert zahlreiche, teils kritische Sicherheitslücken in diversen Produkten aus. IT-Verantwortliche sollten aktiv werden.

- Link

—

Patchday Adobe: Schadcode-Attacken auf After Effects & Co. möglich

Verschiedene Anwendungen von Adobe sind verwundbar. Sicherheitsupdates schließen mehrere Lücken.

- Link

—

Patchday Microsoft: Internet-Explorer-Komponente ermöglicht Attacken

Microsoft hat wichtige Sicherheitspatches für unter anderem Azure, Exchange Server und Windows veröffentlicht. Es gibt bereits Angriffe.

- Link

—

Citrix schließt Sicherheitslücken in Netscaler ADC und Gateway und weitere

Citrix hat Sicherheitsupdates zum Ausbessern von Schwachstellen in Netscaler ADC, Gateway und Session Recording herausgegeben.

- Link

—

Monitoring-Software Icinga: Updates schließen kritische Sicherheitslücke

In Monitoring-Software Icinga klafft eine kritische Sicherheitslücke bei der Zertifikatsüberprüfung. Updates stehen bereit, um sie zu stopfen.

- Link

—

Dell SmartFabric OS10: Angreifer können Schadcode ausführen

Dells Netzwerkbetriebssystem SmartFabric OS10 ist verwundbar. Angreifer können an mehreren Softwareschwachstellen ansetzen.

- Link

—

SAP Patchday: Acht neue Sicherheitslücken, davon eine hochriskant

Admins können etwas entspannter auf den aktuellen SAP-Patchday schauen: Von acht neuen Sicherheitslücken gilt lediglich eine als hohes Risiko.

- Link

—

Veeam Backup Enterprise Manager: Unbefugte Zugriffe durch Angreifer möglich

Ein wichtiges Sicherheitsupdate schützt Veeam Backup Enterprise Manager vor möglichen Attacken.

- 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	0.955250000	0.994630000	Link
CVE-2023-6895	0.925010000	0.990900000	Link
CVE-2023-6553	0.949860000	0.993780000	Link
CVE-2023-6019	0.932040000	0.991600000	Link
CVE-2023-6018	0.911590000	0.989940000	Link
CVE-2023-52251	0.947690000	0.993490000	Link
CVE-2023-4966	0.970550000	0.998130000	Link
CVE-2023-49103	0.947920000	0.993510000	Link
CVE-2023-48795	0.962520000	0.995840000	Link
CVE-2023-47246	0.962070000	0.995770000	Link
CVE-2023-46805	0.962030000	0.995760000	Link
CVE-2023-46747	0.972770000	0.998940000	Link
CVE-2023-46604	0.969640000	0.997770000	Link
CVE-2023-4542	0.941060000	0.992620000	Link
CVE-2023-43208	0.974790000	0.999770000	Link
CVE-2023-43177	0.961030000	0.995560000	Link
CVE-2023-42793	0.970830000	0.998230000	Link
CVE-2023-41892	0.905460000	0.989430000	Link
CVE-2023-41265	0.920970000	0.990560000	Link
CVE-2023-38205	0.958720000	0.995200000	Link
CVE-2023-38203	0.964750000	0.996360000	Link
CVE-2023-38146	0.920950000	0.990560000	Link
CVE-2023-38035	0.974360000	0.999600000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.968430000	0.997420000	Link
CVE-2023-3519	0.965540000	0.996610000	Link
CVE-2023-35082	0.963840000	0.996150000	Link
CVE-2023-35078	0.967840000	0.997250000	Link
CVE-2023-34993	0.973050000	0.999010000	Link
CVE-2023-34634	0.926130000	0.991000000	Link
CVE-2023-34362	0.969380000	0.997700000	Link
CVE-2023-34039	0.935360000	0.991980000	Link
CVE-2023-3368	0.930810000	0.991490000	Link
CVE-2023-33246	0.973040000	0.999010000	Link
CVE-2023-32315	0.973320000	0.999140000	Link
CVE-2023-32235	0.910390000	0.989820000	Link
CVE-2023-30625	0.954240000	0.994450000	Link
CVE-2023-30013	0.966660000	0.996900000	Link
CVE-2023-29300	0.967820000	0.997240000	Link
CVE-2023-29298	0.968380000	0.997410000	Link
CVE-2023-28432	0.906870000	0.989560000	Link
CVE-2023-28343	0.962760000	0.995900000	Link
CVE-2023-28121	0.927310000	0.991110000	Link
CVE-2023-27524	0.970490000	0.998110000	Link
CVE-2023-27372	0.973760000	0.999350000	Link
CVE-2023-27350	0.969220000	0.997650000	Link
CVE-2023-26469	0.958860000	0.995220000	Link
CVE-2023-26360	0.962010000	0.995750000	Link
CVE-2023-26035	0.969120000	0.997620000	Link
CVE-2023-25717	0.950620000	0.993870000	Link
CVE-2023-25194	0.967670000	0.997200000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.961940000	0.995740000	Link
CVE-2023-24489	0.972890000	0.998960000	Link
CVE-2023-23752	0.949040000	0.993660000	Link
CVE-2023-23397	0.902750000	0.989300000	Link
CVE-2023-23333	0.963300000	0.996030000	Link
CVE-2023-22527	0.970570000	0.998140000	Link
CVE-2023-22518	0.963120000	0.995990000	Link
CVE-2023-22515	0.973100000	0.999040000	Link
CVE-2023-21839	0.933960000	0.991830000	Link
CVE-2023-21554	0.955110000	0.994590000	Link
CVE-2023-20887	0.970370000	0.998050000	Link
CVE-2023-1698	0.916400000	0.990200000	Link
CVE-2023-1671	0.962610000	0.995850000	Link
CVE-2023-0669	0.971930000	0.998600000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 13 Nov 2024

[NEU] [hoch] Intel Prozessor (Xeon): Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Intel Prozessor ausnutzen, um einen Denial of Service Angriff durchzuführen und sich erhöhte Rechte zu verschaffen.

- Link

—

Wed, 13 Nov 2024

[NEU] [hoch] Microsoft Azure: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Microsoft Azure ausnutzen, um seine Privilegien zu erhöhen oder beliebigen Code auszuführen.

- Link

—

Wed, 13 Nov 2024

[NEU] [hoch] Microsoft DeveloperTools: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Microsoft Visual Studio Code, Microsoft Visual Studio 2022 und Microsoft Windows ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen und einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Wed, 13 Nov 2024

[NEU] [hoch] Intel Firmware: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Intel Firmware ausnutzen, um seine Privilegien zu erhöhen, vertrauliche Informationen preiszugeben und einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Wed, 13 Nov 2024

[NEU] [hoch] GitLab: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um seine Privilegien zu erhöhen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand zu erzeugen oder einen Cross-Site-Scripting-Angriff durchzuführen.

- Link

—

Wed, 13 Nov 2024

[NEU] [hoch] Microsoft SQL Server: Mehrere Schwachstellen ermöglichen Codeausführung

Ein Angreifer kann mehrere Schwachstellen in Microsoft SQL Server ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 13 Nov 2024

[NEU] [hoch] Fortinet FortiClient für macOS und Windows: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Fortinet FortiClient für macOS und Windows ausnutzen, um beliebigen Programmcode auszuführen, Daten zu manipulieren oder seine Rechte zu erweitern.

- Link

—

Wed, 13 Nov 2024

[NEU] [hoch] Microsoft LightGBM und TorchGeo: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft LightGBM und Torch-

Geo ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Wed, 13 Nov 2024

[NEU] [kritisch] Microsoft Windows: Mehrere Schwachstellen

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

—

Wed, 13 Nov 2024

[NEU] [hoch] Google Chrome: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.
- Link

—

Wed, 13 Nov 2024

[NEU] [hoch] Ivanti Endpoint Manager: Mehrere Schwachstellen ermöglichen Codeausführung

Ein Angreifer kann mehrere Schwachstellen in Ivanti Endpoint Manager ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Wed, 13 Nov 2024

[NEU] [hoch] Ivanti Connect Secure: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Ivanti Connect Secure, Ivanti Policy Secure und Ivanti Secure Access Client ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, einen Denial-of-Service Zustand zu erzeugen und Daten zu modifizieren
- Link

—

Wed, 13 Nov 2024

[NEU] [UNGEPATCHT] [kritisch] D-LINK DWR 2000M 5G CPE Router: Mehrere Schwachstellen

Ein Angreifer aus dem lokalen Netzwerk kann mehrere Schwachstellen in D-LINK DWR 2000M 5G CPE Routern ausnutzen, um den Brute-Force Schutz der Anmeldung zu umgehen und anschließend beliebigen Programmcode auszuführen.
- Link

—

Wed, 13 Nov 2024

[NEU] [hoch] Icinga: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Icinga ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 13 Nov 2024

[NEU] [hoch] Rockwell Automation FactoryTalk: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Rockwell Automation FactoryTalk View ME und FactoryTalk Updater ausnutzen, um Sicherheitsvorkehrungen zu umgehen, seine Rechte zu erweitern, Informationen offenzulegen oder Code auszuführen.

- Link

—

Wed, 13 Nov 2024

[NEU] [hoch] Citrix NetScaler ADC und NetScaler Gateway: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Citrix Systems ADC und Citrix Systems NetScaler ausnutzen, um beliebigen Programmcode auszuführen einen Denial of Service zu verursachen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 13 Nov 2024

[NEU] [hoch] Apache CloudStack: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Apache CloudStack ausnutzen, um Zugriffskontrollen zu umgehen und somit erhöhte Rechte zu erlangen, einen Denial-of-Service-Zustand zu erzeugen und vertrauliche Informationen offenzulegen.

- Link

—

Wed, 13 Nov 2024

[UPDATE] [hoch] Bluetooth Spezifikation: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Bluetooth Chipsätzen zahlreicher Hersteller ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 13 Nov 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Wed, 13 Nov 2024

[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen

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

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
11/13/2024	[Security Updates for Microsoft Visual Studio Products (November 2024)]	critical
11/13/2024	[RHEL 9 : thunderbird (RHSA-2024:9552)]	critical
11/13/2024	[RHEL 9 : krb5 (RHSA-2024:9547)]	critical
11/13/2024	[RHEL 9 : firefox (RHSA-2024:9554)]	critical
11/13/2024	[Ubuntu 14.04 LTS : zlib vulnerability (USN-7107-1)]	critical
11/13/2024	[FreeBSD : icinga2 – TLS Certificate Validation Bypass (0a82bc4d-a129-11ef-8351-589cfc0f81b0)]	critical
11/13/2024	[FreeBSD : Matrix clients – mxc uri validation in js sdk (574f7bc9-a141-11ef-84e9-901b0e9408dc)]	critical
11/13/2024	[FreeBSD : FreeBSD – Unbounded allocation in ctl(4) CAM Target Layer (8caa5d60-a174-11ef-9a62-002590c1f29c)]	critical
11/13/2024	[Siemens (CVE-2024-50557)]	critical
11/13/2024	[Oracle Linux 8 / 9 : Unbreakable Enterprise kernel (ELSA-2024-12815)]	high
11/13/2024	[Mozilla Thunderbird < 128.4.3]	high
11/13/2024	[Mozilla Thunderbird < 128.4.3]	high

Datum	Schwachstelle	Bewertung
11/13/2024	[Mozilla Thunderbird < 132.0.1]	high
11/13/2024	[Mozilla Thunderbird < 132.0.1]	high
11/13/2024	[RHEL 9 : libsoup (RHSA-2024:9572)]	high
11/13/2024	[RHEL 9 : libsoup (RHSA-2024:9559)]	high
11/13/2024	[RHEL 8 : libsoup (RHSA-2024:9525)]	high
11/13/2024	[RHEL 8 : libsoup (RHSA-2024:9566)]	high
11/13/2024	[RHEL 8 : libsoup (RHSA-2024:9524)]	high
11/13/2024	[RHEL 8 : libsoup (RHSA-2024:9573)]	high
11/13/2024	[RHEL 9 : tigervnc (RHSA-2024:9579)]	high
11/13/2024	[Ubuntu 24.04 LTS : Linux kernel vulnerabilities (USN-7089-4)]	high
11/13/2024	[FreeBSD : FreeBSD – Certificate revocation list fetch(1) option fails (ce0f52e1-a174-11ef-9a62-002590c1f29c)]	high
11/13/2024	[RHEL 9 : tigervnc (RHSA-2024:9601)]	high
11/13/2024	[Amazon Linux 2 : python38-pip (ALASPYTHON3.8-2024-015)]	high
11/13/2024	[Amazon Linux 2 : python38 (ALASPYTHON3.8-2024-016)]	high
11/13/2024	[Amazon Linux 2 : libreoffice (ALASLIBREOFFICE-2024-005)]	high
11/13/2024	[Amazon Linux 2 : firefox (ALASFIREFOX-2024-032)]	high
11/13/2024	[Oracle Linux 8 : tigervnc (ELSA-2024-9540)]	high
11/13/2024	[Jenkins plugins Multiple Vulnerabilities (2024-11-13)]	high
11/13/2024	[IBM WebSphere eXtreme Scale 8.6.1.0 < 8.6.1.6 (7175229)]	high
11/13/2024	[Siemens (CVE-2024-50572)]	high
11/13/2024	[Siemens (CVE-2024-50310)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Wed, 13 Nov 2024

Siemens Energy Omnivise T3000 8.2 SP3 Privilege Escalation / File Download

Siemens Energy Omnivise T3000 version 8.2 SP3 suffers from local privilege escalation, cleartext storage of passwords in configuration and log files, file system access allowing for arbitrary file download, and IP whitelist bypass.

- Link

—

” “Wed, 13 Nov 2024

TX Text Control .NET Server For ASP.NET Arbitrary File Read / Write

TX Text Control .NET Server For ASP.NET has an issue where it was possible to change the configured system path for reading and writing files in the underlying operating system with privileges of the user running a web application.

- Link

—

” “Wed, 13 Nov 2024

Palo Alto Expedition 1.2.91 Remote Code Execution

This Metasploit module lets you obtain remote code execution in Palo Alto Expedition versions 1.2.91 and below. The first vulnerability, CVE-2024-5910, allows to reset the password of the admin user, and the second vulnerability, CVE-2024-9464, is an authenticated OS command injection. In a default installation, commands will get executed in the context of www-data. When credentials are provided, this module will only exploit the second vulnerability. If no credentials are provided, the module will first try to reset the admin password and then perform the OS command injection.

- Link

—

” “Mon, 11 Nov 2024

HASOMED Elefant / Elefant Software Updater Data Exposure / Privilege Escalation

HASOMED Elefant versions prior to 24.04.00 and Elefant Software Updater versions prior to 1.4.2.1811 suffer from having an unprotected exposed firebird database, unprotected FHIR API, multiple local privilege escalation, and hardcoded service password vulnerabilities.

- Link

—

” “Mon, 11 Nov 2024

WSO2 4.0.0 / 4.1.0 / 4.2.0 Shell Upload

WS02 versions 4.0.0, 4.1.0, and 4.2.0 are susceptible to remote code execution via an arbitrary file

upload vulnerability.

- Link

—

” “Thu, 07 Nov 2024

WordPress Meetup 0.1 Authentication Bypass

WordPress Meetup plugin versions 0.1 and below suffer from an authentication bypass vulnerability.

- Link

—

” “Thu, 07 Nov 2024

CyberPanel upgrademysqlstatus Arbitrary Command Execution

Proof of concept remote command execution exploit for CyberPanel versions prior to 5b08cd6.

- Link

—

” “Thu, 07 Nov 2024

TestRail CLI FieldsParser eval Injection

While parsing test result XML files with the TestRail CLI, the presence of certain TestRail-specific fields can cause untrusted data to flow into an eval() statement, leading to arbitrary code execution. In order to exploit this, an attacker would need to be able to cause the TestRail CLI to parse a malicious XML file. Normally an attacker with this level of control would already have other avenues of gaining code execution.

- Link

—

” “Tue, 05 Nov 2024

ABB Cylon Aspect 3.08.00 Off-By-One

A vulnerability was identified in a ABB Cylon Aspect version 3.08.00 where an off-by-one error in array access could lead to undefined behavior and potential denial of service. The issue arises in a loop that iterates over an array using a less than or equals to condition, allowing access to an out-of-bounds index. This can trigger errors or unexpected behavior when processing data, potentially crashing the application. Successful exploitation of this vulnerability can lead to a crash or disruption of service, especially if the script handles large data sets.

- Link

—

” “Mon, 04 Nov 2024

Sysax Multi Server 6.99 SSH Denial Of Service

Sysax Multi Server version 6.9.9 suffers from an SSH related denial of service vulnerability.

- Link

—

” “Mon, 04 Nov 2024

Sysax Multi Server 6.99 Cross Site Scripting

Sysax Multi Server version 6.9.9 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 04 Nov 2024

IBM Security Verify Access 32 Vulnerabilities

IBM Security Verify Access versions prior to 10.0.8 suffer from authentication bypass, reuse of private keys, local privilege escalation, weak settings, outdated libraries, missing password, hardcoded secrets, remote code execution, missing authentication, null pointer dereference, and lack of privilege separation vulnerabilities.

- Link

—

” “Mon, 04 Nov 2024

IBM Security Verify Access Appliance Insecure Transit / Hardcoded Passwords

IBM Security Verify Access Appliance suffers from multiple insecure transit vulnerabilities, hardcoded passwords, and uninitialized variables. ibmsecurity versions prior to 2024.4.5 are affected.

- Link

—

” “Mon, 04 Nov 2024

ESET NOD32 Antivirus 18.0.12.0 Unquoted Service Path

ESET NOD32 Antivirus version 18.0.12.0 suffers from an unquoted service path vulnerability.

- Link

—

” “Mon, 04 Nov 2024

SQLite3 generate_series Stack Buffer Underflow

SQLite3 suffers from a stack buffer underflow condition in seriesBestIndex in the generate_series extension.

- Link

—

” “Mon, 04 Nov 2024

Linux khugepaged Race Conditions

khugepaged in Linux races with rmap-based zap, races with GUP-fast, and fails to call MMU notifiers.

- Link

—

” “Fri, 01 Nov 2024

Ping Identity PingIDM 7.5.0 Query Filter Injection

Ping Identity PingIDM versions 7.0.0 through 7.5.0 enabled an attacker with read access to the User collection, to abuse API query filters in order to obtain managed and/or internal user’s passwords in

either plaintext or encrypted variants, based on configuration. The API clearly prevents the password in either plaintext or encrypted to be retrieved by any other means, as this field is set as protected under the User object. However, by injecting a malicious query filter, using password as the field to be filtered, an attacker can perform a blind brute-force on any victim's user password details (encrypted object or plaintext string).

- Link

—

" "Fri, 01 Nov 2024

ABB Cylon Aspect 3.08.01 File Upload MD5 Checksum Bypass

ABB Cylon Aspect version 3.08.01 has a vulnerability in caldavInstall.php, caldavInstallAgendav.php, and caldavUpload.php files, where the presence of an EXPERTMODE parameter activates a badassMode feature. This mode allows an unauthenticated attacker to bypass MD5 checksum validation during file uploads. By enabling badassMode and setting the skipChecksum parameter, the system skips integrity verification, allowing attackers to upload or install altered CalDAV zip files without authentication. This vulnerability permits unauthorized file modifications, potentially exposing the system to tampering or malicious uploads.

- Link

—

" "Fri, 01 Nov 2024

Packet Storm New Exploits For October, 2024

This archive contains all of the 128 exploits added to Packet Storm in October, 2024.

- Link

—

" "Fri, 01 Nov 2024

SmartAgent 1.1.0 Remote Code Execution

SmartAgent version 1.1.0 suffers from an unauthenticated remote code execution vulnerability in youtubeInfo.php.

- Link

—

" "Fri, 01 Nov 2024

SmartAgent 1.1.0 Server-Side Request Forgery

SmartAgent version 1.1.0 suffers from a server-side request forgery vulnerability.

- Link

—

" "Fri, 01 Nov 2024

SmartAgent 1.1.0 SQL Injection

SmartAgent version 1.1.0 suffers from multiple unauthenticated remote SQL injection vulnerabilities.

- Link

—

” “Thu, 31 Oct 2024

WordPress Automatic 3.92.0 Path Traversal / Server-Side Request Forgery

WordPress Automatic plugin versions 3.92.0 and below proof of concept exploit that demonstrates path traversal and server-side request forgery vulnerabilities.

- Link

—

” “Thu, 31 Oct 2024

Qualitor 8.24 Server-Side Request Forgery

Qualitor versions 8.24 and below suffer from an unauthenticated server-side request forgery vulnerability.

- Link

—

” “Thu, 31 Oct 2024

CyberPanel Command Injection

Proof of concept exploit for a command injection vulnerability in CyberPanel. This vulnerability enables unauthenticated attackers to inject and execute arbitrary commands on vulnerable servers by sending crafted OPTIONS HTTP requests to /dns/getresetstatus and /ftp/getresetstatus endpoints, potentially leading to full system compromise. Versions prior to 1c0c6cb appear to be affected.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Wed, 13 Nov 2024

ZDI-24-1510: Ivanti Endpoint Manager GetComputerID SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1509: Ivanti Endpoint Manager vulscan Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1508: Ivanti Endpoint Manager GetDetectedVulnerabilitiesDataTable SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1507: Ivanti Endpoint Manager ROI SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1506: Ivanti Endpoint Manager serverStorage SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1505: Ivanti Endpoint Manager GetFilePath Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1504: Ivanti Endpoint Manager TestAllowedSQL SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1503: Ivanti Endpoint Manager OnSaveToDB Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1502: Ivanti Endpoint Manager Report_RunPatch SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1501: Ivanti Endpoint Manager EFile Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1500: Ivanti Endpoint Manager DBDR SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1499: Ivanti Endpoint Manager PatchHistory SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1498: Ivanti Endpoint Manager Report_Run SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1497: Ivanti Endpoint Manager MP_QueryDetail SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1496: Ivanti Endpoint Manager Report_Run2 SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1495: Ivanti Endpoint Manager MP_QueryDetail2 SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1494: Ivanti Endpoint Manager GetCountForQuery SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1493: Ivanti Endpoint Manager MP_VistaReport SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1492: Ivanti Avalanche WLAvalancheService TV_FP Infinite Loop Denial-of-Service Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1491: Ivanti Avalanche WLAvalancheService TV_FC Infinite Loop Denial-of-Service Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1490: Ivanti Avalanche WLAvalancheService TV_FN Infinite Loop Denial-of-Service Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1489: Ivanti Avalanche WLAvalancheService TV_FP Null Pointer Dereference Denial-of-Service Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1488: Ivanti Avalanche WLAvalancheService TV_FN Null Pointer Dereference Denial-of-Service Vulnerability

- Link

—

” “Wed, 13 Nov 2024

ZDI-24-1487: Ivanti Secure Access Client Pulse Secure Service Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1486: (0Day) G DATA Total Security Incorrect Permission Assignment Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1485: (0Day) Trimble SketchUp Viewer SKP File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1484: (0Day) Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1483: (0Day) Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1482: (0Day) Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1481: (0Day) Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1480: (0Day) Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1479: (0Day) Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1478: (0Day) Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1477: (0Day) Trimble SketchUp Viewer SKP File Parsing Out-Of-Bounds Read Remote Code

Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1476: (0Day) Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1475: (0Day) Trimble SketchUp Viewer SKP File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1474: (0Day) Trimble SketchUp Pro SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1473: (0Day) Trimble SketchUp SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1472: Veeam Backup Enterprise Manager AuthorizeByVMwareSsoToken Improper Certificate Validation Authentication Bypass Vulnerability

- Link

—

” “Mon, 11 Nov 2024

ZDI-24-1471: Panda Security Dome PSANHost Link Following Local Privilege Escalation Vulnerability

- Link

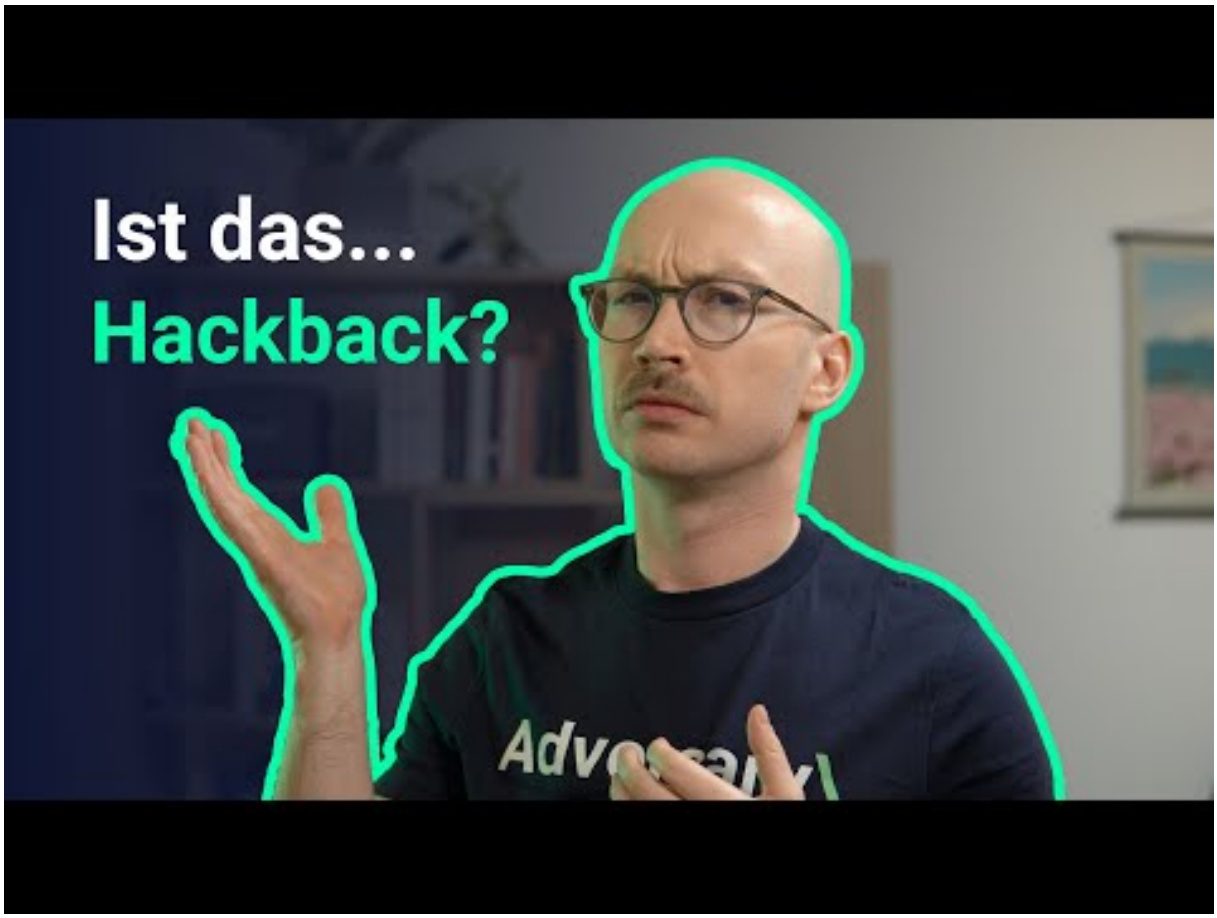
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Sophos spielt die UNO Reverse Karte (+ Redline Stealer)



Zum Youtube Video

6 Cyberangriffe: (Nov)

Datum	Opfer	Land	Information
2024-11-09	Sheboygan	[USA]	Link
2024-11-09	Berufsförderungswerk Oberhausen	[DEU]	Link
2024-11-09	Southern Oregon Veterinary Specialty Center (SOVSC)	[USA]	Link
2024-11-07	Département des Hautes-Pyrénées	[FRA]	Link
2024-11-07	Ahold Delhaize	[USA]	Link
2024-11-05	Lojas Marisa	[BRA]	Link
2024-11-05	Wexford County	[USA]	Link
2024-11-05	Ridgewood Schools	[USA]	Link
2024-11-04	Avis de Torino	[ITA]	Link
2024-11-03	Washington state courts	[USA]	Link
2024-11-03	La Sauvegarde	[FRA]	Link
2024-11-02	Memorial Hospital and Manor	[USA]	Link
2024-11-02	Kumla kommun	[SWE]	Link
2024-11-01	South East Technological University (SETU)	[IRL]	Link

7 Ransomware-Erpressungen: (Nov)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-11-14	[Popular Life Insurance]	sarcoma	Link
2024-11-14	[Micon National]	sarcoma	Link
2024-11-14	[Kelowna Springs]	sarcoma	Link
2024-11-13	[stalyhill-inf.tameside.sch.uk]	blacksuit	Link
2024-11-13	[AXEON 360]	ciphbit	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-11-13	[COOPERATIVA TELEFONICA DE CALAFATE LTD.]	BrainCipher	Link
2024-11-13	[G-One Auto Parts de México S.A. de C.V.]	BrainCipher	Link
2024-11-13	[Schmack]	hunters	Link
2024-11-13	[Sercomm]	hunters	Link
2024-11-13	[midstatesindustrial.com]	threeam	Link
2024-11-13	[nanolive.ch 2.0]	apt73	Link
2024-11-05	[formosacpa.com.tw]	kairos	Link
2024-11-05	[clayplattefamily.com]	kairos	Link
2024-11-05	[askyouraccountant.com]	kairos	Link
2024-11-11	[pmrcenter.com]	kairos	Link
2024-11-13	[kansasrmc.com]	kairos	Link
2024-11-13	[Value Dental Center]	everest	Link
2024-11-13	[Artistic Family Dental]	everest	Link
2024-11-13	[Asaro Dental Aesthetics]	everest	Link
2024-11-13	[Axpr Valve Science]	killsec	Link
2024-11-12	[American Associated Pharmacies]	embargo	Link
2024-11-12	[Giggle Finance]	killsec	Link
2024-11-12	[Orange County Pathology Medical Group]	raworld	Link
2024-11-12	[SK Gas]	raworld	Link
2024-11-03	[Medigroup.ca]	ransomhub	Link
2024-11-12	[steppingstonesd.org]	blacksuit	Link
2024-11-12	[Hillandale Farms]	akira	Link
2024-11-12	[jst.es]	blacksuit	Link
2024-11-12	[jarrellimc.com]	blacksuit	Link
2024-11-06	[Banco de Fomento Internacional]	lynx	Link
2024-11-11	[TaxPros of Clermont]	lynx	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-11-11	[National Institute of Administration]	killsec	Link
2024-11-07	[DSZ]	lynx	Link
2024-11-07	[Future Metals]	lynx	Link
2024-11-07	[Plowman Craven]	lynx	Link
2024-11-11	[Supply Technologies]	blacksuit	Link
2024-11-11	[Maxxis International]	blacksuit	Link
2024-11-11	[potteau.be]	ransomhub	Link
2024-11-11	[Followmont TransportPty Ltd]	akira	Link
2024-11-11	[dezinecorp.com]	blacksuit	Link
2024-11-11	[Amourgis & Associates]	hunters	Link
2024-11-11	[Dietzgen Corporation]	hunters	Link
2024-11-01	[nynewspapers.com]	ransomhub	Link
2024-11-11	[comarchs.com]	ransomhub	Link
2024-11-11	[tolbertlegal.com]	ransomhub	Link
2024-11-10	[Banco Sucredito Regional S.A.U.]	hunters	Link
2024-11-10	[OxyHealth]	killsec	Link
2024-11-10	[Immuno Laboratories, Inc]	bianlian	Link
2024-11-05	[bitquail.com]	ransomhub	Link
2024-11-09	[ATSG, Inc]	bianlian	Link
2024-11-09	[Mizuno (USA)]	bianlian	Link
2024-11-09	[Palmisano & Goodman, P.A.]	bianlian	Link
2024-11-09	[Finger Beton Unternehmensgruppe]	meow	Link
2024-11-09	[Karman Inc]	meow	Link
2024-11-09	[Siltech (siltechcorp.local)]	lynx	Link
2024-11-09	[emefarmario.com.br]	apt73	Link
2024-11-09	[Granite School District]	rhysida	Link
2024-11-09	[WimCoCorp]	lynx	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-11-09	[NEBRASKALAND]	lynx	Link
2024-11-08	[MENZIES CNAC (Jardine Aviation Services, Agility)]	spacebears	Link
2024-11-08	[bartleycorp.com]	ransomhub	Link
2024-11-08	[interlabel.be]	ransomhub	Link
2024-11-07	[del-electric.com]	ransomhub	Link
2024-11-08	[liftkits4less.com]	apt73	Link
2024-11-08	[www.lamaisonducitron.com]	apt73	Link
2024-11-08	[www.baldinger-ag.ch]	apt73	Link
2024-11-07	[Marisa S.A]	medusa	Link
2024-11-08	[www.assurified.com]	apt73	Link
2024-11-08	[www.botiga.com.uy]	apt73	Link
2024-11-08	[Healthcare Management Systems]	bianlian	Link
2024-11-08	[MedElite Group]	everest	Link
2024-11-07	[nelconinc.biz]	ransomhub	Link
2024-11-07	[www.fdc.ie]	ransomhub	Link
2024-11-07	[www.cenergica.com]	ransomhub	Link
2024-11-07	[www.bluco.com]	ransomhub	Link
2024-11-07	[naj.ae]	darkvault	Link
2024-11-07	[Equator Worldwide]	meow	Link
2024-11-07	[Lexco]	meow	Link
2024-11-07	[europe-qualité]	incransom	Link
2024-11-07	[Winnebago Public School Foundation]	interlock	Link
2024-11-05	[Alliance Technical Group]	medusa	Link
2024-11-06	[Jomar Electrical Contractors]	medusa	Link
2024-11-06	[Howell Electric Inc]	medusa	Link
2024-11-06	[www.msdl.ca]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-11-07	[Postcard Mania]	play	Link
2024-11-07	[New Law]	hunters	Link
2024-11-06	[klinkamkurpark]	helldown	Link
2024-11-06	[AMERICANVENTURE]	helldown	Link
2024-11-06	[CSIKBS]	helldown	Link
2024-11-06	[SANJACINTOCOUNY]	helldown	Link
2024-11-06	[brandenburgerplumbing.com]	ransomhub	Link
2024-11-06	[arcoexc.com]	ransomhub	Link
2024-11-06	[Lincoln University]	meow	Link
2024-11-06	[Cape Cod Regional Technical High School (capetech.us)]	fog	Link
2024-11-06	[GSR Andrade Architects (gsr-andrade.com)]	fog	Link
2024-11-05	[metroelectric.com]	ransomhub	Link
2024-11-05	[sector5.ro]	ransomhub	Link
2024-11-05	[Paragon Plastics]	play	Link
2024-11-05	[Delfin Design & Manufacturing]	play	Link
2024-11-05	[Smitty’s Supply]	play	Link
2024-11-05	[S & W Kitchens]	play	Link
2024-11-05	[Dome Construction]	play	Link
2024-11-06	[Interoute agency]	lynx	Link
2024-11-06	[LmayInteroute agency]	lynx	Link
2024-11-05	[pacificglazing.com]	ransomhub	Link
2024-11-05	[nwhealthporter.com]	ransomhub	Link
2024-11-05	[wexfordcounty.org]	embargo	Link
2024-11-05	[ebrso]	qilin	Link
2024-11-05	[Model Die & Mold]	lynx	Link
2024-11-04	[mh-m.org]	embargo	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-11-05	[Falco Sult]	bianlian	Link
2024-11-05	[apoyoconsultoria.com]	ransomhub	Link
2024-11-05	[Webb Institute]	incransom	Link
2024-11-05	[Fylde Coast Academy Trust]	rhysida	Link
2024-11-04	[sundt.com]	ransomhub	Link
2024-11-04	[Memorial Hospital & Manor]	embargo	Link
2024-11-02	[Scolari]	dragonforce	Link
2024-11-05	[McMillan Electric Company]	medusa	Link
2024-11-04	[maxdata.com.br]	ransomhub	Link
2024-11-04	[goodline.com.au]	ransomhub	Link
2024-11-04	[kenanasugarcompany.com]	ransomhub	Link
2024-11-04	[www.schweiker.de]	ransomhub	Link
2024-11-04	[www.drbutlerandassociates.com]	ransomhub	Link
2024-11-04	[www.mssupply.com]	ransomhub	Link
2024-11-04	[fullfordelectric.com]	ransomhub	Link
2024-11-04	[College of Business - Tanzania]	hellcat	Link
2024-11-04	[Ministry of Education - Jordan]	hellcat	Link
2024-11-04	[Schneider Electric - France]	hellcat	Link
2024-11-04	[International University of Sarajevo]	medusa	Link
2024-11-04	[Whitaker Construction Group]	medusa	Link
2024-11-04	[European External Action Service (EEAS)]	hunters	Link
2024-11-04	[csucontracting.com]	ransomhub	Link
2024-11-04	[redphoenixconstruction.com]	ransomhub	Link
2024-11-04	[Air Specialists Heating & Air Conditioning]	hunters	Link
2024-11-03	[krigerconstruction.com]	ransomhub	Link
2024-11-03	[caseconstruction.com]	ransomhub	Link
2024-11-03	[lambertstonecommercial.com]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-11-04	[Doctor 24x7]	killsec	Link
2024-11-03	[Hemubo]	hunters	Link
2024-11-03	[Elad municipality]	handala	Link
2024-11-03	[Russell Law Firm, LLC]	bianlian	Link
2024-11-03	[L & B Transport, L.L.C.]	bianlian	Link
2024-11-03	[guardianhc]	stormous	Link
2024-11-02	[bravodigitaltrader.co.uk]	ransomhub	Link
2024-11-02	[SVP Worldwide]	blacksuit	Link
2024-11-02	[Sumitomo]	killsec	Link
2024-11-01	[DieTech North America]	qilin	Link
2024-11-01	[www.fatboysfleetandauto.com]	ransomhub	Link
2024-11-01	[lighthouseelectric.com]	ransomhub	Link
2024-11-01	[JS McCarthy Printers]	play	Link
2024-11-01	[CGR Technologies]	play	Link
2024-11-01	[lumiplan.com]	cactus	Link
2024-11-01	[United Sleep Diagnostics]	medusa	Link
2024-11-01	[eap.gr]	ransomhub	Link
2024-11-01	[vikurverk.is]	lockbit3	Link
2024-11-01	[mirandaproduce.com.ve]	lockbit3	Link
2024-11-01	[Cerp Bretagne Nord]	hunters	Link
2024-11-01	[Hope Valley Recovery]	rhysida	Link
2024-11-01	[lsst.ac]	cactus	Link
2024-11-01	[MCNA Dental]	everest	Link
2024-11-01	[Arctrade]	everest	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.