Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240716

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

Admin-Lücke bedroht Palo Alto Networks Migration-Tool Expedition

Verschiedene Cybersicherheitsprodukte von Palo Alto Networks sind verwundbar. Sicherheitsupdates sind verfügbar.

- Link

—

Sicherheitslücken GitLab: Angreifer können Softwareentwicklung manipulieren

GitLab Community Edition und Enterprise Edition sind verwundbar. Die Entwickler raten zu einem zügigen Update.

- Link

—

Webkonferenzen: Zoom dichtet acht Sicherheitslücken ab

In der Webkonferenz-Software klaffen mehrere Sicherheitslücken, eine davon hochriskant. Updates dichten sie ab.

- Link

—

Nvidia: Angreifer können Schadcode durch Grafikkartentreiber-Lücke schieben

Es sind Attacken auf Windows-PCs mit unter anderem GeForce- oder RTX-Grafikkarten möglich. Berichte zu Angriffen gibt es aber noch nicht.

- Link

—

Cisco: Secure Boot bei einigen Routern umgehbar, Anfälligkeit auf RADIUS-Lücke

Angreifer können einigen Cisco-Routern manipulierte Software unterschieben. Die Entwickler prüfen, welche Geräte von der RADIUS-Lücke betroffen sind.

- Link

—

Juniper Networks: 46 Sicherheitswarnungen veröffentlicht

Juniper Networks hat zu seinem regulären Update-Tag 46 Sicherheitsmitteilungen veröffentlicht. Admins sollten die Updates zügig installieren.

- Link

—

VMware stopft SQL-Injection-Lücke in Aria Automation

Angreifer können eine Schwachstelle in VMware Aria Automation missbrauchen, um eigene Befehle mittels SQL-Injection einzuschleusen. Updates stehen bereit.

- Link

—

Blast-RADIUS: Sicherheitslücke im Netzwerkprotokoll RADIUS veröffentlicht

Lange bekannte Schwachstellen können dem RADIUS-Protokoll zum Verhängnis werden, das vor allem im Enterprise-Umfeld in sehr vielen Netzwerken eingesetzt wird.

- Link

—

Patchday Fortinet: FortiAIOps und FortiOS gegen mögliche Attacken gerüstet

Angreifer können mehrere Produkte von Fortinet ins Visier nehmen und unter anderem sensible Daten einsehen.

- Link

—

OpenSSH: Weitere RegreSSHion-artige Lücke entdeckt

Die RegreSSHion-Lücke ermöglichte Angreifern Root-Zugriff. Ein IT-Forscher hat eine weitere ähnliche Lücke in OpenSSH von RHEL 9 und Abkömmlingen entdeckt.

- 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	0.962510000	0.995510000	Link
CVE-2023-6895	0.922010000	0.989840000	Link
CVE-2023-6553	0.936860000	0.991410000	Link
CVE-2023-5360	0.911260000	0.989000000	Link
CVE-2023-52251	0.930900000	0.990790000	Link
CVE-2023-4966	0.971290000	0.998140000	Link
CVE-2023-49103	0.953130000	0.993800000	Link
CVE-2023-48795	0.965740000	0.996390000	Link
CVE-2023-47246	0.951210000	0.993440000	Link
CVE-2023-46805	0.958670000	0.994760000	Link
CVE-2023-46747	0.972630000	0.998620000	Link
CVE-2023-46604	0.963510000	0.995760000	Link
CVE-2023-4542	0.921170000	0.989730000	Link
CVE-2023-43208	0.959520000	0.994930000	Link
CVE-2023-43177	0.962660000	0.995540000	Link
CVE-2023-42793	0.970960000	0.997990000	Link
CVE-2023-41265	0.905890000	0.988620000	Link
CVE-2023-39143	0.940070000	0.991790000	Link
CVE-2023-38646	0.906240000	0.988660000	Link
CVE-2023-38205	0.954590000	0.994090000	Link
CVE-2023-38203	0.966000000	0.996440000	Link
CVE-2023-38146	0.905210000	0.988570000	Link
CVE-2023-38035	0.974190000	0.999420000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.963940000	0.995870000	Link
CVE-2023-3519	0.965360000	0.996280000	Link
CVE-2023-35082	0.968030000	0.997050000	Link
CVE-2023-35078	0.968330000	0.997140000	Link
CVE-2023-34993	0.972880000	0.998740000	Link
CVE-2023-34960	0.929370000	0.990640000	Link
CVE-2023-34634	0.927960000	0.990430000	Link
CVE-2023-34468	0.906650000	0.988680000	Link
CVE-2023-34362	0.969920000	0.997630000	Link
CVE-2023-34039	0.944490000	0.992380000	Link
CVE-2023-3368	0.933870000	0.991110000	Link
CVE-2023-33246	0.972790000	0.998700000	Link
CVE-2023-32315	0.973570000	0.999070000	Link
CVE-2023-30625	0.943100000	0.992170000	Link
CVE-2023-30013	0.962250000	0.995430000	Link
CVE-2023-29300	0.968380000	0.997160000	Link
CVE-2023-29298	0.943170000	0.992190000	Link
CVE-2023-28771	0.902140000	0.988400000	Link
CVE-2023-28343	0.949510000	0.993180000	Link
CVE-2023-28121	0.909760000	0.988880000	Link
CVE-2023-27524	0.970570000	0.997820000	Link
CVE-2023-27372	0.972890000	0.998750000	Link
CVE-2023-27350	0.970130000	0.997670000	Link
CVE-2023-26469	0.935230000	0.991250000	Link
CVE-2023-26360	0.962310000	0.995470000	Link
CVE-2023-26035	0.967100000	0.996760000	Link
CVE-2023-25717	0.956860000	0.994470000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-25194	0.969960000	0.997640000	Link
CVE-2023-2479	0.963740000	0.995820000	Link
CVE-2023-24489	0.973310000	0.998950000	Link
CVE-2023-23752	0.954250000	0.994020000	Link
CVE-2023-23397	0.901800000	0.988370000	Link
CVE-2023-23333	0.964220000	0.995920000	Link
CVE-2023-22527	0.970550000	0.997810000	Link
CVE-2023-22518	0.965070000	0.996180000	Link
CVE-2023-22515	0.973330000	0.998960000	Link
CVE-2023-21839	0.957210000	0.994540000	Link
CVE-2023-21554	0.950840000	0.993360000	Link
CVE-2023-20887	0.970320000	0.997760000	Link
CVE-2023-1671	0.962480000	0.995500000	Link
CVE-2023-0669	0.969330000	0.997420000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 15 Jul 2024

[UPDATE] [hoch] IBM WebSphere Application Server: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in IBM WebSphere Application Server ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Mon, 15 Jul 2024

[UPDATE] [hoch] OpenSSH: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in OpenSSH ausnutzen, um beliebigen Programmcode mit root Rechten auszuführen.

- Link

—

Mon, 15 Jul 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service zu verursachen.

- Link

—

Mon, 15 Jul 2024

[UPDATE] [hoch] less: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Mon, 15 Jul 2024

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer oder ein lokaler authentifizierter Angreiferkann mehrere Schwachstellen in git ausnutzen, um beliebigen Programmcode auszuführen und und die Sicherheitsmaßnahmen zu umgehen.

- Link

—

Mon, 15 Jul 2024

[UPDATE] [hoch] Ghostscript: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Ghostscript ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen.

- Link

—

Mon, 15 Jul 2024

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

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

- Link

—

Fri, 12 Jul 2024

[UPDATE] [hoch] Apache HttpComponents: Schwachstelle ermöglicht Täuschung des Nutzers

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache HttpComponents ausnutzen, um den Nutzer zu täuschen.

- Link

—

Fri, 12 Jul 2024

[UPDATE] [hoch] Drupal: Mehrere Schwachstellen

Ein entfernter, authentisierter oder anonymer Angreifer kann mehrere Schwachstellen in Drupal ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen, um Daten zu manipulieren, um einen Denial of Service Zustand herbeizuführen und um beliebigen Code auszuführen.

- Link

—

Fri, 12 Jul 2024

[UPDATE] [hoch] GNU libc: Schwachstelle ermöglicht Codeausführung

Ein Angreifer kann eine Schwachstelle in GNU libc ausnutzen, um einen Denial-of-Service-Zustand zu verursachen, Code auszuführen oder seine Privilegien zu erweitern.

- Link

—

Fri, 12 Jul 2024

[NEU] [hoch] Fabasoft Folio: Schwachstelle ermöglicht Codeausführung

Ein Angreifer aus einem angrenzenden Netzwerk kann eine Schwachstelle in Fabasoft Folio ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 12 Jul 2024

[UPDATE] [hoch] Python: Schwachstelle ermöglicht Manipulation

Ein Angreifer kann eine Schwachstelle in Python ausnutzen, um HTTP Anfragen zu manipulieren.

- Link

—

Fri, 12 Jul 2024

[UPDATE] [hoch] Python: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Python ausnutzen, um Dateien zu manipulieren und Schutzmechanismen zu umgehen.

- Link

—

Fri, 12 Jul 2024

[UPDATE] [hoch] Python: Schwachstelle ermöglicht nicht spezifizierten Angriff

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Python ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen oder Informationen offenzulegen.

- Link

—

Fri, 12 Jul 2024

[UPDATE] [hoch] Python: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit Benutzerrechten

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Python ausnutzen, um beliebigen Programmcode mit Benutzerrechten auszuführen.

- Link

—

Fri, 12 Jul 2024

[UPDATE] [kritisch] Python: Schwachstelle ermöglicht Codeausführung

Ein Angreifer kann eine Schwachstelle in Python ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 12 Jul 2024

[UPDATE] [hoch] Python: Schwachstelle ermöglicht Privilegieneskalation

Ein lokaler Angreifer kann eine Schwachstelle in Python ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Fri, 12 Jul 2024

[UPDATE] [hoch] Python: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Python ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Fri, 12 Jul 2024

[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen ermöglichen HTTP Response Splitting

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um einen Response Splitting Angriff durchzuführen.

- Link

—

Fri, 12 Jul 2024

[UPDATE] [hoch] Python: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Python ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder vertrauliche Informationen offenzulegen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
7/15/2024	[EulerOS 2.0 SP10 : ruby (EulerOS-SA-2024-1897)]	critical
7/15/2024	[EulerOS 2.0 SP10 : ruby (EulerOS-SA-2024-1921)]	critical
7/15/2024	[EulerOS 2.0 SP10 : git (EulerOS-SA-2024-1906)]	critical
7/15/2024	[EulerOS 2.0 SP10 : git (EulerOS-SA-2024-1882)]	critical
7/15/2024	[RHEL 9 : git-lfs (RHSA-2024:4543)]	high
7/15/2024	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6898-1)]	high
7/15/2024	[EulerOS 2.0 SP10 : xorg-x11-server (EulerOS-SA-2024-1901)]	high
7/15/2024	[EulerOS 2.0 SP10 : kernel (EulerOS-SA-2024-1887)]	high
7/15/2024	[EulerOS 2.0 SP10 : less (EulerOS-SA-2024-1912)]	high
7/15/2024	[EulerOS 2.0 SP10 : curl (EulerOS-SA-2024-1902)]	high
7/15/2024	[EulerOS 2.0 SP10 : expat (EulerOS-SA-2024-1881)]	high
7/15/2024	[EulerOS 2.0 SP10 : sssd (EulerOS-SA-2024-1898)]	high
7/15/2024	[EulerOS 2.0 SP10 : glibc (EulerOS-SA-2024-1883)]	high
7/15/2024	[EulerOS 2.0 SP10 : kernel (EulerOS-SA-2024-1911)]	high
7/15/2024	[EulerOS 2.0 SP10 : expat (EulerOS-SA-2024-1905)]	high
7/15/2024	[EulerOS 2.0 SP10 : python-idna (EulerOS-SA-2024-1918)]	high
7/15/2024	[EulerOS 2.0 SP10 : systemd (EulerOS-SA-2024-1899)]	high
7/15/2024	[EulerOS 2.0 SP10 : xorg-x11-server (EulerOS-SA-2024-1925)]	high
7/15/2024	[EulerOS 2.0 SP10 : mod_http2 (EulerOS-SA-2024-1891)]	high
7/15/2024	[EulerOS 2.0 SP10 : httpd (EulerOS-SA-2024-1886)]	high
7/15/2024	[EulerOS 2.0 SP10 : sssd (EulerOS-SA-2024-1922)]	high
7/15/2024	[EulerOS 2.0 SP10 : systemd (EulerOS-SA-2024-1923)]	high
7/15/2024	[EulerOS 2.0 SP10 : libxml2 (EulerOS-SA-2024-1889)]	high

Datum	Schwachstelle	Bewertung
7/15/2024	[EulerOS 2.0 SP10 : less (EulerOS-SA-2024-1888)]	high
7/15/2024	[EulerOS 2.0 SP10 : libxml2 (EulerOS-SA-2024-1913)]	high
7/15/2024	[EulerOS 2.0 SP10 : mod_http2 (EulerOS-SA-2024-1915)]	high
7/15/2024	[EulerOS 2.0 SP10 : curl (EulerOS-SA-2024-1878)]	high
7/15/2024	[EulerOS 2.0 SP10 : httpd (EulerOS-SA-2024-1910)]	high
7/15/2024	[EulerOS 2.0 SP10 : glibc (EulerOS-SA-2024-1907)]	high
7/15/2024	[EulerOS 2.0 SP10 : python-idna (EulerOS-SA-2024-1894)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Mon, 15 Jul 2024

Geoserver Unauthenticated Remote Code Execution

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

- Link

—

” “Mon, 15 Jul 2024

WordPress PZ Frontend Manager 1.0.5 Cross Site Request Forgery

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

- Link

—

” “Mon, 15 Jul 2024

Havoc C2 0.7 Server-Side Request Forgery

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

—

” “Mon, 15 Jul 2024

Confluence Template Injection Remote Code Execution

Atlassian Confluence suffers from a template injection vulnerability that leads to remote code execution. This repository has three go-exploit implementations of CVE-2023-22527 that execute their payload without touching disk.
- Link

—

” “Thu, 11 Jul 2024

Atlassian Confluence Administrator Code Macro Remote Code Execution

This Metasploit module exploits an authenticated administrator-level vulnerability in Atlassian Confluence, tracked as CVE-2024-21683. The vulnerability exists due to the Rhino script engine parser evaluating tainted data from uploaded text files. This facilitates arbitrary code execution. This exploit will authenticate, validate user privileges, extract the underlying host OS information, then trigger remote code execution. All versions of Confluence prior to 7.17 are affected, as are many versions up to 8.9.0.
- Link

—

” “Thu, 11 Jul 2024

LumisXP 16.1.x Cross Site Scripting

LumisXP versions 15.0.x through 16.1.x suffer from a cross site scripting vulnerability in XsltResultControllerHtml.jsp.
- Link

—

” “Thu, 11 Jul 2024

LumisXP 16.1.x Cross Site Scripting

LumisXP versions 15.0.x through 16.1.x suffer from a cross site scripting vulnerability in UrlAccessibilityEvaluation.jsp.
- Link

—

” “Thu, 11 Jul 2024

LumisXP 16.1.x Cross Site Scripting

LumisXP versions 15.0.x through 16.1.x suffer from a cross site scripting vulnerability in main.jsp
- Link

—

” “Thu, 11 Jul 2024

LumisXP 16.1.x Hardcoded Credentials / IDOR

LumisXP versions 15.0.x through 16.1.x have a hardcoded privileged identifier that allows attackers to bypass authentication and access internal pages and other sensitive information.

- Link

—

” “Thu, 11 Jul 2024

WordPress Poll Maker 5.3.2 SQL Injection

WordPress Poll Maker plugin version 5.3.2 suffers from a remote SQL injection vulnerability.

- Link

—

” “Thu, 11 Jul 2024

ESET NOD32 Antivirus 17.2.7.0 Unquoted Service Path

ESET NOD32 Antivirus version 17.2.7.0 suffers from an unquoted service path vulnerability.

- Link

—

” “Wed, 10 Jul 2024

Microsoft SharePoint Remote Code Execution

This archive contains three proof of concepts exploit for multiple Microsoft SharePoint remote code execution vulnerabilities.

- Link

—

” “Tue, 09 Jul 2024

Ivanti EPM RecordGoodApp SQL Injection / Remote Code Execution

Ivanti Endpoint Manager (EPM) 2022 SU5 and prior versions are susceptible to an unauthenticated SQL injection vulnerability which can be leveraged to achieve unauthenticated remote code execution.

- Link

—

” “Mon, 08 Jul 2024

WordPress Poll 2.3.6 SQL Injection

WordPress Poll plugin version 2.3.6 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 08 Jul 2024

VMWare Aria Operations For Networks Command Injection

VMWare Aria Operations for Networks (vRealize Network Insight) is vulnerable to command injection when accepting user input through the Apache Thrift RPC interface. This is a proof of concept exploit.

- Link

—

” “Mon, 08 Jul 2024

Veeam Backup Enterprise Manager Authentication Bypass

Veeam Backup Enterprise Manager authentication bypass proof of concept exploit. Versions prior to 12.1.2.172 are vulnerable.

- Link

—

” “Mon, 08 Jul 2024

Veeam Recovery Orchestrator Authentication Bypass

Veeam Recovery Orchestrator authentication bypass proof of concept exploit.

- Link

—

” “Mon, 08 Jul 2024

Telerik Report Server Deserialization / Authentication Bypass

Telerik Report Server deserialization and authentication bypass exploit chain that makes use of the vulnerabilities noted in CVE-2024-4358 and CVE-2024-1800.

- Link

—

” “Mon, 08 Jul 2024

Progress WhatsUp Gold WriteDatafile Unauthenticated Remote Code Execution

Progress WhatsUp Gold WriteDatafile unauthenticated remote code execution proof of concept exploit.

- Link

—

” “Mon, 08 Jul 2024

Progress WhatsUp Gold GetFileWithoutZip Unauthenticated Remote Code Execution

Progress WhatsUp Gold GetFileWithoutZip unauthenticated remote code execution proof of concept exploit.

- Link

—

” “Mon, 08 Jul 2024

Progress WhatsUp Gold SetAdminPassword Privilege Escalation

Progress WhatsUp Gold SetAdminPassword local privilege escalation proof of concept exploit.

- Link

—

” “Mon, 08 Jul 2024

ResidenceCMS 2.10.1 Cross Site Scripting

ResidenceCMS versions 2.10.1 and below suffer from a persistent cross site scripting vulnerability.

- Link

—

” “Mon, 08 Jul 2024

PMS 2024 1.0 SQL Injection

PMS 2024 version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 08 Jul 2024

Simple Online Banking System 1.0 SQL Injection

Simple Online Banking System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Mon, 08 Jul 2024

Microsoft Office 365 Remote Code Execution

Microsoft Office 365 appears susceptible to macro code execution that can result in remote code execution.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Mon, 15 Jul 2024

ZDI-24-899: Centreon testServiceExistence SQL Injection Remote Code Execution Vulnerability

- Link

—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Wieder mal die Lieferkette: polyfill.io wird verkauft, spielt Schadcode aus.

Zum Youtube Video

6 Cyberangriffe: (Jul)

Datum	Opfer	Land	Information
2024-07-13	AKG	[DEU]	Link
2024-07-10	Jaboatão dos Guararapes	[BRA]	Link
2024-07-10	Sibanye Stillwater	[ZAF]	Link
2024-07-10	District scolaire de Goshen	[USA]	Link
2024-07-09	Clay County Courthouse	[USA]	Link
2024-07-09	Ville de Mahina	[FRA]	Link
2024-07-07	Frankfurter University of Applied Sciences (UAS)	[DEU]	Link
2024-07-04	La Ville d'Ans	[BEL]	Link
2024-07-03	E.S.E. Salud Yopal	[COL]	Link
2024-07-03	Florida Department of Health	[USA]	Link
2024-07-03	Southwest Tennessee Community College (SWTCC)	[USA]	Link
2024-07-02	Hong Kong Institute of Architects	[HKG]	Link
2024-07-02	Apex	[USA]	Link
2024-07-01	Hiap Seng Industries	[SGP]	Link
2024-07-01	Monroe County government	[USA]	Link

7 Ransomware-Erpressungen: (Jul)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-15	[Nuevatel]	dunghill	Link
2024-07-15	[Innovalve Bio Medical]	handala	Link
2024-07-09	[www.baiminstitute.org]	ransomhub	Link
2024-07-13	[integraservices]	mallox	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-14	[XENAPP-GLOBER]	mallox	Link
2024-07-15	[Gramercy Surgery Center]	everest	Link
2024-07-15	[posiplus.com]	blackbasta	Link
2024-07-15	[hpecds.com]	blackbasta	Link
2024-07-15	[Amino Transport]	akira	Link
2024-07-15	[Goede, DeBoest & Cross, PLLC.]	rhysida	Link
2024-07-15	[Sheba Medical Center]	handala	Link
2024-07-15	[usdermpartners.com]	blackbasta	Link
2024-07-15	[atos.com]	blackbasta	Link
2024-07-15	[Gibbs Hurley Chartered Accountants]	hunters	Link
2024-07-15	[ComNet Communications]	hunters	Link
2024-07-15	[MS Ultrasonic Technology Group]	hunters	Link
2024-07-15	[RZO]	hunters	Link
2024-07-15	[thompsoncreek.com_wa]	blackbasta	Link
2024-07-15	[northernsafety.com_wa]	blackbasta	Link
2024-07-15	[upcli.com]	cloak	Link
2024-07-15	[greenlightbiosciences.com]	abyss	Link
2024-07-15	[valleylandtitleco.com - UPD]	donutleaks	Link
2024-07-14	[luzan5.com]	blackout	Link
2024-07-14	[BrownWinick]	rhysida	Link
2024-07-14	[Texas Alcohol & Drug Testing Service]	bianlian	Link
2024-07-13	[a-g.com - data publication 38gb (150K)]	blacksuit	Link
2024-07-13	[gbhs.org Publication 51gb]	blacksuit	Link
2024-07-13	[Kenya Urban Roads Authority]	hunters	Link
2024-07-13	[Carigali Hess Operating Company]	hunters	Link
2024-07-13	[gbhs.org 07/12 Publication 51gb]	blacksuit	Link
2024-07-01	[The Coffee Bean & Tea Leaf]	incransom	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-01	[State of Alabama - Alabama Department Of Education]	incransom	Link
2024-07-02	[ARISTA]	spacebears	Link
2024-07-12	[Preferred IT Group]	bianlian	Link
2024-07-08	[Wagner-Meinert]	ransomexx	Link
2024-07-12	[painproclinics.com]	ransomcortex	Link
2024-07-02	[www.zepter.de]	ransomhub	Link
2024-07-11	[www.riteaid.com]	ransomhub	Link
2024-07-03	[olympusgrp.com]	dispossessor	Link
2024-07-12	[www.donaanita.com]	ransomcortex	Link
2024-07-12	[perfeitaplastica.com.br]	ransomcortex	Link
2024-07-12	[www.respirarlondrina.com.br]	ransomcortex	Link
2024-07-11	[Hyperice]	play	Link
2024-07-11	[diligentusa.com]	embargo	Link
2024-07-11	[Image Microsystems]	blacksuit	Link
2024-07-11	[www.lynchaluminum.com]	ransomhub	Link
2024-07-11	[www.eurostrand.de]	ransomhub	Link
2024-07-11	[www.netavent.dk]	ransomhub	Link
2024-07-11	[Financoop]	akira	Link
2024-07-11	[Sigma]	akira	Link
2024-07-11	[Sonol (Gas Stations)]	handala	Link
2024-07-11	[www.bfcsolutions.com]	ransomhub	Link
2024-07-11	[Texas Electric Cooperatives]	play	Link
2024-07-11	[The 21st Century Energy Group]	play	Link
2024-07-11	[T P C I]	play	Link
2024-07-10	[City of Cedar Falls]	blacksuit	Link
2024-07-10	[P448]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-10	[Beowulfchain]	vanirgroup	Link
2024-07-10	[Qinao]	vanirgroup	Link
2024-07-10	[Athlon]	vanirgroup	Link
2024-07-10	[Usina Alta Mogiana S/A]	akira	Link
2024-07-09	[Inland Audio Visual]	akira	Link
2024-07-09	[Indika Energy]	hunters	Link
2024-07-08	[Excelsior Orthopaedics]	monti	Link
2024-07-09	[Heidmar]	akira	Link
2024-07-03	[REPLIGEN]	incransom	Link
2024-07-08	[Raffmetal Spa]	dragonforce	Link
2024-07-08	[Allied Industrial Group]	akira	Link
2024-07-08	[Esedra]	akira	Link
2024-07-08	[Federated Co-operatives]	akira	Link
2024-07-02	[Guhring USA]	incransom	Link
2024-07-06	[noab.nl]	lockbit3	Link
2024-07-07	[Strauss Brands]	medusa	Link
2024-07-07	[Harry Perkins Institute of medical research]	medusa	Link
2024-07-07	[Viasat]	medusa	Link
2024-07-07	[Olympus Group]	medusa	Link
2024-07-07	[MYC Media]	rhysida	Link
2024-07-06	[a-g.com 7/10/24 - data publication 38gb (150K)]	blacksuit	Link
2024-07-03	[baiminstitute.org]	ransomhub	Link
2024-07-05	[The Wacks Law Group]	qilin	Link
2024-07-05	[pomalca.com.pe]	qilin	Link
2024-07-05	[Center for Human Capital Innovation (centerforhci.org)]	incransom	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-05	[waupacacounty-wi.gov]	incransom	Link
2024-07-05	[waupaca.wi.us]	incransom	Link
2024-07-04	[ws-stahl.eu]	lockbit3	Link
2024-07-04	[homelandvinyl.com]	lockbit3	Link
2024-07-04	[eicher.in]	lockbit3	Link
2024-07-05	[National Health Laboratory Services]	blacksuit	Link
2024-07-04	[Un Museau]	spacebears	Link
2024-07-03	[Haylem]	spacebears	Link
2024-07-04	[Elyria Foundry]	play	Link
2024-07-04	[Texas Recycling]	play	Link
2024-07-04	[INDA’s]	play	Link
2024-07-04	[Innerspec Technologies]	play	Link
2024-07-04	[Prairie Athletic Club]	play	Link
2024-07-04	[Fareri Associates]	play	Link
2024-07-04	[Island Transportation Corp.]	bianlian	Link
2024-07-04	[Legend Properties, Inc.]	bianlian	Link
2024-07-04	[Transit Mutual Insurance Corporation]	bianlian	Link
2024-07-03	[hcri.edu]	ransomhub	Link
2024-07-04	[Coquitlam Concrete]	hunters	Link
2024-07-04	[Multisuns Communication]	hunters	Link
2024-07-04	[gerard-perrier.com]	embargo	Link
2024-07-04	[Abileneisd.org]	cloak	Link
2024-07-03	[sequelglobal.com]	darkvault	Link
2024-07-03	[Explomin]	akira	Link
2024-07-03	[Alimac]	akira	Link
2024-07-03	[badel1862.hr]	blackout	Link
2024-07-03	[ramservices.com]	underground	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-03	[foremedia.net]	darkvault	Link
2024-07-03	[www.swcs-inc.com]	ransomhub	Link
2024-07-03	[valleylandtitleco.com]	donutleaks	Link
2024-07-02	[merrymanhouse.org]	lockbit3	Link
2024-07-02	[fairfieldmemorial.org]	lockbit3	Link
2024-07-02	[www.daesangamerica.com]	ransomhub	Link
2024-07-02	[P1 Technologies]	akira	Link
2024-07-02	[Conexus Medstaff]	akira	Link
2024-07-02	[Salton]	akira	Link
2024-07-01	[www.sfmedical.de]	ransomhub	Link
2024-07-02	[WheelerShip]	hunters	Link
2024-07-02	[Grand Rapids Gravel]	dragonforce	Link
2024-07-02	[Franciscan Friars of the Atonement]	dragonforce	Link
2024-07-02	[Elite Fitness]	dragonforce	Link
2024-07-02	[Gray & Adams]	dragonforce	Link
2024-07-02	[Vermont Panurgy]	dragonforce	Link
2024-07-01	[floridahealth.gov]	ransomhub	Link
2024-07-01	[www.nttdata.ro]	ransomhub	Link
2024-07-01	[Super Gardens]	dragonforce	Link
2024-07-01	[Hampden Veterinary Hospital]	dragonforce	Link
2024-07-01	[Indonesia Terkoneksi]	BrainCipher	Link
2024-07-01	[SYNERGY PEANUT]	akira	Link
2024-07-01	[Ethypharm]	underground	Link
2024-07-01	[latinusa.co.id]	lockbit3	Link
2024-07-01	[kbc-zagreb.hr]	lockbit3	Link
2024-07-01	[maxcess-logistics.com]	killsec	Link
2024-07-01	[Independent Education System]	handala	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-01	[Bartlett & Weigle Co. LPA.]	hunters	Link

8 Quellen

8.1 Quellenverzeichnis

1) Cyberwatch - https://github.com/Casualtek/Cyberwatch
2) Ransomware.live - https://data.ransomware.live
3) Heise Security Alerts! - https://www.heise.de/security/alerts/
4) First EPSS - https://www.first.org/epss/
5) BSI WID - https://wid.cert-bund.de/
6) Tenable Plugins - https://www.tenable.com/plugins/
7) Exploit - packetstormsecurity.com
8) 0-Day - https://www.zerodayinitiative.com/rss/published/
9) Die Hacks der Woche - https://martinhaunschmid.com/videos

9 Impressum

Herausgeber:
Marlon Hübner
Brückenstraße 3
57629 Höchstenbach

E-Mail
info@cyberwald.com

Cyberwald ist ein privates, nicht-kommerzielles Projekt zur Förderung des Bewusstseins für Cybersicherheit.