Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240507

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

Trend Micro Antivirus One: Codeschmuggel im macOS-Scanner möglich

Trend Micros Antivirus One lässt sich durch eine Schwachstelle unter macOS beliebigen Code unterjubeln. Ein Update steht bereit.

- Link

—

Sicherheitsupdates: Angreifer können IP-Telefone von Cisco ausspionieren

Admins sollten zeitnah die abgesicherte Firmware für Ciscos IP-Telefone der Serien 6800, 7800 und 8800 installieren.

- Link

—

CISA warnt: Microsoft Smartscreen- und Gitlab-Sicherheitsleck werden angegriffen

Die US-Cybersicherheitsbehörde CISA hat Angriffe auf eine Lücke im Microsoft Smartscreen und auf eine Gitlab-Schwachstelle gesichtet.

- Link

—

Sicherheitsupdates: Angreifer können WLAN-Gateways von Aruba kompromittieren

Wichtige Patches schließen mehrere Schwachstellen in Mobillity Conductor, Mobility Controllers, WLAN Gateways und SD-WAN Gateways von Aruba.

- Link

—

Acronis Cyber Protect: Rechteausweitung und Informationsleck möglich

Sicherheitslecks in Acronis Cyber Protect ermöglichen die Ausweitung der Rechte und Informationsabfluss. Updates korrigieren das.

- Link

—

Qnap schließt NAS-Sicherheitslücken aus Hacker-Wettbewerb Pwn2Own

NAS-Modelle von Qnap sind verwundbar. Nun hat der Hersteller Sicherheitsupdates für das Betriebssystem und Apps veröffentlicht.

- Link

—

Sicherheitsupdates: Angreifer können GitLab-Accounts übernehmen

Wichtige Sicherheitsupdates schließen mehrere Sicherheitslücken in GitLab. Der Anbieter rät zu einem zügigen Update.

- Link

—

Cross-Site Scripting: Sicherheitslücken in pfSense ermöglichen Admin-Cookieklau

Die Open-Source-Firewall pfSense hat mehrere Löcher, durch die Angreifer eigenen Javascript-Code einschleusen können. Updates sind verfügbar.

- Link

—

Cisco: Angreifer plazieren mithilfe neuer 0-Day-Lücke Hintertüren auf Firewalls

Zwei geschickt gestaltete Hintertüren auf Geräten mit Ciscos ASA- und FTD-System überleben Reboots und Systemupdates. Viele Details sind noch unklar.

- Link

—

AMD Radeon-Grafiktreiber: Update schließt Codeschmuggel-Lücke

AMD hat Updates für Radeon-Grafiktreiber für DirectX 11 veröffentlicht. Sie schließen Sicherheitslücken, durch die Angreifer Schadcode einschleusen können.

- 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	0.953820000	0.993450000	Link
CVE-2023-6895	0.901600000	0.987700000	Link
CVE-2023-6553	0.922860000	0.989330000	Link
CVE-2023-5360	0.967230000	0.996510000	Link
CVE-2023-4966	0.966680000	0.996330000	Link
CVE-2023-48795	0.962250000	0.995070000	Link
CVE-2023-47246	0.943770000	0.991770000	Link
CVE-2023-46805	0.965580000	0.996060000	Link
CVE-2023-46747	0.972430000	0.998380000	Link
CVE-2023-46604	0.972730000	0.998490000	Link
CVE-2023-43177	0.964020000	0.995570000	Link
CVE-2023-42793	0.971040000	0.997760000	Link
CVE-2023-39143	0.950730000	0.992980000	Link
CVE-2023-38646	0.913020000	0.988520000	Link
CVE-2023-38205	0.922000000	0.989230000	Link
CVE-2023-38203	0.971170000	0.997850000	Link
CVE-2023-38035	0.974130000	0.999300000	Link
CVE-2023-36845	0.965540000	0.996050000	Link
CVE-2023-3519	0.911860000	0.988460000	Link
CVE-2023-35082	0.959780000	0.994560000	Link
CVE-2023-35078	0.966030000	0.996160000	Link
CVE-2023-34993	0.966220000	0.996200000	Link
CVE-2023-34960	0.934040000	0.990610000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34634	0.918830000	0.988980000	Link
CVE-2023-34362	0.955650000	0.993790000	Link
CVE-2023-34039	0.934640000	0.990650000	Link
CVE-2023-3368	0.908410000	0.988150000	Link
CVE-2023-33246	0.973220000	0.998760000	Link
CVE-2023-32315	0.974090000	0.999260000	Link
CVE-2023-32235	0.911650000	0.988440000	Link
CVE-2023-30625	0.945200000	0.992090000	Link
CVE-2023-30013	0.960350000	0.994670000	Link
CVE-2023-29300	0.970030000	0.997380000	Link
CVE-2023-29298	0.948030000	0.992500000	Link
CVE-2023-28771	0.914030000	0.988600000	Link
CVE-2023-28432	0.935270000	0.990730000	Link
CVE-2023-28121	0.945870000	0.992170000	Link
CVE-2023-27524	0.970430000	0.997530000	Link
CVE-2023-27372	0.973780000	0.999030000	Link
CVE-2023-27350	0.970720000	0.997640000	Link
CVE-2023-26469	0.933870000	0.990570000	Link
CVE-2023-26360	0.962720000	0.995190000	Link
CVE-2023-26035	0.969280000	0.997130000	Link
CVE-2023-25717	0.957880000	0.994200000	Link
CVE-2023-25194	0.969190000	0.997100000	Link
CVE-2023-2479	0.963600000	0.995440000	Link
CVE-2023-24489	0.974200000	0.999330000	Link
CVE-2023-23752	0.932080000	0.990360000	Link
CVE-2023-23397	0.926450000	0.989850000	Link
CVE-2023-23333	0.963260000	0.995350000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-22527	0.974360000	0.999420000	Link
CVE-2023-22518	0.966340000	0.996250000	Link
CVE-2023-22515	0.972060000	0.998190000	Link
CVE-2023-21839	0.958250000	0.994270000	Link
CVE-2023-21554	0.959160000	0.994450000	Link
CVE-2023-20887	0.961910000	0.995000000	Link
CVE-2023-1671	0.968860000	0.997010000	Link
CVE-2023-0669	0.969750000	0.997290000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 06 May 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

—

Mon, 06 May 2024

[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen

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

- Link

—

Mon, 06 May 2024

[NEU] [UNGEPATCHT] [kritisch] Linksys Router: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Linksys Router ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 06 May 2024

[NEU] [hoch] Trend Micro AntiVirus: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in Trend Micro AntiVirus ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 06 May 2024

[UPDATE] [hoch] strongSwan: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in strongSwan ausnutzen, um Sicherheitsvorkehrungen zu umgehen und einen Denial of Service Zustand herzustellen.

- Link

—

Mon, 06 May 2024

[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen

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

- Link

—

Mon, 06 May 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in strongSwan und Ubuntu Linux ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Mon, 06 May 2024

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

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

- Link

—

Mon, 06 May 2024

[UPDATE] [hoch] Heimdal: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Heimdal, Samba, MIT Kerberos und FreeBSD Project FreeBSD OS ausnutzen, um einen Denial of Service Angriff durchzuführen, und um beliebigen Code auszuführen.

- Link

—

Mon, 06 May 2024

[UPDATE] [hoch] strongSwan: Schwachstelle ermöglicht Codeausführung und DoS

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in strongSwan ausnutzen, um einen Denial of Service zu verursachen und beliebigen Programmcode auszuführen.

- Link

—

Mon, 06 May 2024

[UPDATE] [hoch] ImageMagick: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in ImageMagick ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Mon, 06 May 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial of Service Zustand herbeizuführen, Informationen offenzulegen, Dateien zu manipulieren oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Mon, 06 May 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, 06 May 2024

[UPDATE] [hoch] IBM DB2: Schwachstelle ermöglicht Privilegieneskalation

Ein lokaler Angreifer kann eine Schwachstelle in IBM DB2 ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Mon, 06 May 2024

[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen

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

- Link

—

Mon, 06 May 2024

[UPDATE] [hoch] Red Hat Enterprise Linux (Pillow): Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux in der Komponente “Pillow” ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 06 May 2024

[UPDATE] [hoch] PostgreSQL JDBC Driver: Schwachstelle ermöglicht SQL-Injection

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PostgreSQL JDBC Driver ausnutzen, um eine SQL-Injection durchzuführen.

- Link

—

Mon, 06 May 2024

[UPDATE] [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, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder einen nicht spezifizierten Angriff durchzuführen.

- Link

—

Mon, 06 May 2024

[UPDATE] [hoch] IBM MQ: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in IBM MQ ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Mon, 06 May 2024

[UPDATE] [hoch] Ruby: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Ruby ausnutzen, um Informationen offenzulegen oder Code auszuführen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
5/6/2024	[Oracle Linux 9 : webkit2gtk3 (ELSA-2024-2126)]	critical
5/6/2024	[Oracle Linux 9 : freerdp (ELSA-2024-2208)]	critical
5/6/2024	[Oracle Linux 9 : qt5-qtbase (ELSA-2024-2276)]	critical
5/6/2024	[Oracle Linux 9 : xorg-x11-server-Xwayland (ELSA-2024-2170)]	critical
5/6/2024	[Oracle Linux 9 : xorg-x11-server (ELSA-2024-2169)]	critical
5/6/2024	[Zebra FX9500 RFID Reader Unrestricted Upload of File with Dangerous Type (CVE-2021-32089)]	critical
5/6/2024	[Oracle Linux 9 : gstreamer1-plugins-base (ELSA-2024-2302)]	high
5/6/2024	[Oracle Linux 9 : mod_http2 (ELSA-2024-2368)]	high
5/6/2024	[Oracle Linux 9 : buildah (ELSA-2024-2245)]	high
5/6/2024	[Oracle Linux 9 : perl (ELSA-2024-2228)]	high
5/6/2024	[Oracle Linux 9 : edk2 (ELSA-2024-2264)]	high
5/6/2024	[Oracle Linux 9 : pmix (ELSA-2024-2199)]	high
5/6/2024	[Oracle Linux 9 : containernetworking-plugins (ELSA-2024-2272)]	high
5/6/2024	[Oracle Linux 9 : libsndfile (ELSA-2024-2184)]	high
5/6/2024	[Oracle Linux 9 : freeglut (ELSA-2024-2366)]	high
5/6/2024	[Oracle Linux 9 : python3.11-cryptography (ELSA-2024-2337)]	high
5/6/2024	[Oracle Linux 9 : mingw-glib2 (ELSA-2024-2528)]	high
5/6/2024	[Oracle Linux 9 : libjpeg-turbo (ELSA-2024-2295)]	high
5/6/2024	[Oracle Linux 9 : grub2 (ELSA-2024-2456)]	high
5/6/2024	[Oracle Linux 9 : tigervnc (ELSA-2024-2298)]	high
5/6/2024	[Oracle Linux 9 : skopeo (ELSA-2024-2239)]	high
5/6/2024	[Oracle Linux 9 : python3.11-urllib3 (ELSA-2024-2159)]	high
5/6/2024	[Oracle Linux 9 : gstreamer1-plugins-bad-free (ELSA-2024-2287)]	high
5/6/2024	[Oracle Linux 9 : gstreamer1-plugins-good (ELSA-2024-2303)]	high

Datum	Schwachstelle	Bewertung
5/6/2024	[Oracle Linux 9 : libX11 (ELSA-2024-2145)]	high
5/6/2024	[Oracle Linux 9 : mingw / components (ELSA-2024-2353)]	high
5/6/2024	[Oracle Linux 9 : harfbuzz (ELSA-2024-2410)]	high
5/6/2024	[Zebra FX9500 RFID Reader Path Traversal (CVE-2020-10875)]	high
5/6/2024	[Zebra Industrial Printers Insufficiently Protected Credentials (CVE-2019-10960)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Mon, 06 May 2024

Systemd Insecure PTY Handling

Systemd-run/run0 allocates user-owned ptys and attaches the slave to high privilege programs without changing ownership or locking the pty slave.

- Link

—

” “Mon, 06 May 2024

Microsoft PlayReady Toolkit

The Microsoft PlayReady toolkit assists with fake client device identity generation, acquisition of license and content keys for encrypted content, and much more. It demonstrates weak content protection in the environment of CANAL+. The proof of concept exploit 3 year old vulnerabilities in CANAL+ STB devices, which make it possible to gain code execution access to target STB devices over an IP network.

- Link

—

” “Mon, 06 May 2024

Docker Privileged Container Kernel Escape

This Metasploit module performs a container escape onto the host as the daemon user. It takes advantage of the SYS_MODULE capability. If that exists and the linux headers are available to compile on the target, then we can escape onto the host.

- Link

—

” “Fri, 03 May 2024

SOPlanning 1.52.00 SQL Injection

SOPlanning version 1.52.00 suffers from a remote SQL injection vulnerability in projects.php.

- Link

—

” “Fri, 03 May 2024

SOPlanning 1.52.00 Cross Site Request Forgery

SOPlanning version 1.52.00 suffers from a cross site request forgery vulnerability in xajax_server.php.

- Link

—

” “Fri, 03 May 2024

SOPlanning 1.52.00 Cross Site Scripting

SOPlanning version 1.52.00 suffers from a cross site scripting vulnerability in groupe_save.php.

- Link

—

” “Thu, 02 May 2024

htmlLawed 1.2.5 Remote Command Execution

htmlLawed versions 1.2.5 and below proof of concept remote command execution exploit.

- Link

—

” “Wed, 01 May 2024

Packet Storm New Exploits For April, 2024

This archive contains all of the 132 exploits added to Packet Storm in April, 2024.

- Link

—

” “Wed, 01 May 2024

Online Tours And Travels Management System 1.0 SQL Injection

Online Tours and Travels Management System version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Tue, 30 Apr 2024

Windows PspBuildCreateProcessContext Double-Fetch / Buffer Overflow

Proof of concept code that demonstrates how the Windows kernel suffers from a privilege escalation vulnerability due to a double-fetch in PspBuildCreateProcessContext that leads to a stack buffer overflow.

- Link

—

” “Tue, 30 Apr 2024

Windows NtQueryInformationThread Double-Fetch / Arbitrary Write

Proof of concept code that demonstrates how the Windows kernel suffers from a privilege escalation vulnerability due to a double-fetch in NtQueryInformationThread that leads to an arbitrary write.

- Link

—

” “Tue, 30 Apr 2024

undefinedExploiting The NT Kernel In 24H2undefined

This is the full Windows privilege escalation exploit produced from the blog Exploiting the NT Kernel in 24H2: New Bugs in Old Code and Side Channels Against KASLR.

- Link

—

” “Tue, 30 Apr 2024

osCommerce 4 Cross Site Scripting

osCommerce version 4 suffers from a cross site scripting vulnerability. This finding is another vector of attack for this issue already discovered by the same researcher in November of 2023.

- Link

—

” “Mon, 29 Apr 2024

Kemp LoadMaster Unauthenticated Command Injection

This Metasploit module exploits an unauthenticated command injection vulnerability in Progress Kemp LoadMaster in the authorization header after version 7.2.48.1. The following versions are patched: 7.2.59.2 (GA), 7.2.54.8 (LTSF), and 7.2.48.10 (LTS).

- Link

—

” “Mon, 29 Apr 2024

Doctor Appointment Management System 1.0 Cross Site Scripting

Doctor Appointment Management System version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 29 Apr 2024

ESET NOD32 Antivirus 17.1.11.0 Unquoted Service Path

ESET NOD32 Antivirus version 17.1.11.0 suffers from an unquoted service path vulnerability.

- Link

—

” “Thu, 25 Apr 2024

PowerVR PMRMMapPMR() Writability Check

PowerVR has a security issue where a writability check in PMRMMapPMR() does not clear

VM_MAYWRITE.

- Link

—

” “Wed, 24 Apr 2024

Apache Solr Backup/Restore API Remote Code Execution

Apache Solr versions 6.0.0 through 8.11.2 and versions 9.0.0 up to 9.4.1 are affected by an unrestricted file upload vulnerability which can result in remote code execution in the context of the user running Apache Solr. When Apache Solr creates a Collection, it will use a specific directory as the classpath and load some classes from it. The backup function of the Collection can export malicious class files uploaded by attackers to the directory, allowing Solr to load custom classes and create arbitrary Java code. Execution can further bypass the Java sandbox configured by Solr, ultimately causing arbitrary command execution.

- Link

—

” “Wed, 24 Apr 2024

Relate Learning And Teaching System SSTI / Remote Code Execution

Relate Learning and Teaching System versions prior to 2024.1 suffers from a server-side template injection vulnerability that leads to remote code execution. This particular finding targets the Batch-Issue Exam Tickets function.

- Link

—

” “Wed, 24 Apr 2024

Nginx 1.25.5 Host Header Validation

Nginx versions 1.25.5 and below appear to have a host header filtering validation bug that could possibly be used for malice.

- Link

—

” “Tue, 23 Apr 2024

FortiNet FortiClient EMS 7.2.2 / 7.0.10 SQL Injection / Remote Code Execution

A remote SQL injection vulnerability exists in FortiNet FortiClient EMS (Endpoint Management Server) versions 7.2.0 through 7.2.2 and 7.0.1 through 7.0.10. FortiClient EMS serves as an endpoint management solution tailored for enterprises, offering a centralized platform for overseeing enrolled endpoints. The SQL injection vulnerability is due to user controller strings which can be sent directly into database queries. FcmDaemon.exe is the main service responsible for communicating with enrolled clients. By default it listens on port 8013 and communicates with FCTDas.exe which is responsible for translating requests and sending them to the database. In the message header of a specific request sent between the two services, the FCTUID parameter is vulnerable to SQL injection. It can be used to enable the xp_cmdshell which can then be used to obtain unauthenticated remote

code execution in the context of NT AUTHORITY\SYSTEM. Upgrading to either 7.2.3, 7.0.11 or above is recommended by FortiNet. It should be noted that in order to be vulnerable, at least one endpoint needs to be enrolled / managed by FortiClient EMS for the necessary vulnerable services to be available.

- Link

—

” “Tue, 23 Apr 2024

GitLens Git Local Configuration Execution

GitKraken GitLens versions prior to 14.0.0 allow an untrusted workspace to execute git commands. A repo may include its own .git folder including a malicious config file to execute arbitrary code. Tested against VSCode 1.87.2 with GitLens 13.6.0 on Ubuntu 22.04 and Windows 10.

- Link

—

” “Tue, 23 Apr 2024

Visual Studio Code Execution

This Metasploit module creates a vsix file which can be installed in Visual Studio Code as an extension. At activation/install, the extension will execute a shell or two. Tested against VSCode 1.87.2 on Ubuntu 22.04.

- Link

—

” “Tue, 23 Apr 2024

Gambio Online Webshop 4.9.2.0 Remote Code Execution

A remote code execution vulnerability in Gambio online webshop versions 4.9.2.0 and below allows remote attackers to run arbitrary commands via an unauthenticated HTTP POST request. The identified vulnerability within Gambio pertains to an insecure deserialization flaw, which ultimately allows an attacker to execute remote code on affected systems. The insecure deserialization vulnerability in Gambio poses a significant risk to affected systems. As it allows remote code execution, adversaries could exploit this flaw to execute arbitrary commands, potentially resulting in complete system compromise, data exfiltration, or unauthorized access to sensitive information.

- Link

—

” “Tue, 23 Apr 2024

Palo Alto Networks PAN-OS Unauthenticated Remote Code Execution

This Metasploit module exploits two vulnerabilities in Palo Alto Networks PAN-OS that allow an unauthenticated attacker to create arbitrarily named files and execute shell commands. Configuration requirements are PAN-OS with GlobalProtect Gateway or GlobalProtect Portal enabled and telemetry collection on (default). Multiple versions are affected. Payloads may take up to one hour to execute, depending on how often the telemetry service is set to run.

- Link
—
”

4.2 0-Days der letzten 5 Tage

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Schadsoftware via offiziellem GitHub Link?

Zum Youtube Video

6 Cyberangriffe: (Mai)

Datum	Opfer	Land	Information
2024-05-05	Wichita	[USA]	Link
2024-05-05	Université de Sienne	[ITA]	Link
2024-05-04	Regional Cancer Center (RCC)	[IND]	Link
2024-05-03	Eucatex (EUCA4)	[BRA]	Link
2024-05-03	Cégep de Lanaudière	[CAN]	Link
2024-05-02	Umeå universitet	[SWE]	Link

7 Ransomware-Erpressungen: (Mai)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-05-05	[SBC Global, Bitfinex, Coinmama, and Rutgers University Part 2 Leak]	flocker	Link
2024-05-07	[Central Florida Equipment]	play	Link
2024-05-07	[High Performance Services]	play	Link
2024-05-07	[Mauritzon]	play	Link
2024-05-07	[Somerville]	play	Link
2024-05-07	[Donco Air]	play	Link
2024-05-07	[Affordable Payroll & Bookkeeping Services]	play	Link
2024-05-07	[Utica Mack]	play	Link
2024-05-07	[KC Scout]	play	Link
2024-05-07	[Sentry Data Management]	play	Link
2024-05-07	[aletech.com.br]	darkvault	Link
2024-05-07	[Young Consulting]	blacksuit	Link
2024-05-06	[Thaayakam LTD]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-05-06	[The Weinstein Firm]	qilin	Link
2024-05-06	[Nikolaus & Hohenadel]	bianlian	Link
2024-05-06	[NRS Healthcare]	ransomhub	Link
2024-05-06	[gammarenax.ch]	lockbit3	Link
2024-05-06	[oraclinical.com]	lockbit3	Link
2024-05-06	[acsistemas.com]	lockbit3	Link
2024-05-06	[cpashin.com]	lockbit3	Link
2024-05-06	[epr-groupe.fr]	lockbit3	Link
2024-05-06	[isee.biz]	lockbit3	Link
2024-05-06	[cdev.gc.ca]	lockbit3	Link
2024-05-06	[netspectrum.ca]	lockbit3	Link
2024-05-06	[qstartlabs.com]	lockbit3	Link
2024-05-06	[syntax-architektur.at]	lockbit3	Link
2024-05-06	[carespring.com]	lockbit3	Link
2024-05-06	[grand-indonesia.com]	lockbit3	Link
2024-05-06	[remagroup.com]	lockbit3	Link
2024-05-06	[telekom.com]	lockbit3	Link
2024-05-06	[aev-iledefrance.fr]	lockbit3	Link
2024-05-06	[elarabygroup.com]	lockbit3	Link
2024-05-06	[thebiglifegroup.com]	lockbit3	Link
2024-05-06	[sonoco.com]	lockbit3	Link
2024-05-06	[ville-bouchemaine.fr]	lockbit3	Link
2024-05-06	[eskarabajo.mx]	darkvault	Link
2024-05-06	[Rafael Viñoly Architects]	blacksuit	Link
2024-05-06	[TRC Talent Solutions]	blacksuit	Link
2024-05-06	[M2E Consulting Engineers]	akira	Link
2024-05-06	[sunray.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-05-06	[eviivo.com]	lockbit3	Link
2024-05-06	[kras.hr]	lockbit3	Link
2024-05-06	[tdt.aero]	lockbit3	Link
2024-05-06	[svenskakyrkan.se]	lockbit3	Link
2024-05-06	[htcinc.com]	lockbit3	Link
2024-05-06	[irc.be]	lockbit3	Link
2024-05-06	[geotechenv.com]	lockbit3	Link
2024-05-06	[ishoppes.com]	lockbit3	Link
2024-05-06	[parat-techology.com]	lockbit3	Link
2024-05-06	[getcloudapp.com]	lockbit3	Link
2024-05-06	[yucatan.gob.mx]	lockbit3	Link
2024-05-06	[arcus.pl]	lockbit3	Link
2024-05-06	[Nestoil]	blacksuit	Link
2024-05-06	[Patterson & Rothwell Ltd]	medusa	Link
2024-05-06	[Boyden]	medusa	Link
2024-05-06	[W.F. Whelan]	medusa	Link
2024-05-05	[SBC Global, Bitfinex, Coinmama, and Rutgers University Part 2]	flocker	Link
2024-05-05	[Seneca Nation Health System]	incransom	Link
2024-05-05	[SBC Global, Bitfinex, Coinmom, and Rutgers University Part 2]	flocker	Link
2024-05-04	[COMPEXLEGAL.COM]	clop	Link
2024-05-04	[ikfhomefinance.com]	darkvault	Link
2024-05-04	[The Islamic Emirat of Afghanistan National Environmental Protection Agency]	ransomhub	Link
2024-05-04	[Accounting Professionals LLC. Price, Breazeale & Chastang]	everest	Link
2024-05-04	[cmactrans.com]	blackbasta	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-05-04	[ids-michigan.com]	blackbasta	Link
2024-05-04	[provencherroy.ca]	blackbasta	Link
2024-05-04	[swisspro.ch]	blackbasta	Link
2024-05-04	[olsonsteel.com]	blackbasta	Link
2024-05-04	[teaspa.it]	blackbasta	Link
2024-05-04	[ayesa.com]	blackbasta	Link
2024-05-04	[synlab.com]	blackbasta	Link
2024-05-04	[active-pcb.com]	blackbasta	Link
2024-05-04	[gai-it.com]	blackbasta	Link
2024-05-04	[Macildowie Associates]	medusa	Link
2024-05-03	[Dr Charles A Evans]	qilin	Link
2024-05-03	[Universidad Nacional Autónoma de México]	ransomhub	Link
2024-05-03	[thelawrencegroup.com]	blackbasta	Link
2024-05-02	[sharik]	stormous	Link
2024-05-02	[tdra]	stormous	Link
2024-05-02	[fanr.gov.ae]	stormous	Link
2024-05-02	[Bayanat]	stormous	Link
2024-05-02	[kidx]	stormous	Link
2024-05-03	[MCS]	qilin	Link
2024-05-03	[Tohlen Building Technology Group]	qilin	Link
2024-05-03	[Stainless Foundry & Engineering]	play	Link
2024-05-02	[Ayoub & associates CPA Firm]	everest	Link
2024-05-02	[www.servicepower.com]	apt73	Link
2024-05-02	[www.credio.eu]	apt73	Link
2024-05-02	[Lopez Hnos]	rhysida	Link
2024-05-02	[GWF Frankenwein]	raworld	Link
2024-05-02	[Reederei Jüngerhans]	raworld	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-05-02	[extraco.ae]	ransomhub	Link
2024-05-02	[watergate]	qilin	Link
2024-05-02	[Imedi L]	akira	Link
2024-05-01	[Azteca Tax Systems]	bianlian	Link
2024-05-01	[Clinica de Salud del Valle de Salinas]	bianlian	Link
2024-05-01	[cochraneglobal.com]	underground	Link
2024-05-01	[UK government]	snatch	Link
2024-05-01	[hookerfurniture.com]	lockbit3	Link
2024-05-01	[alimmigration.com]	lockbit3	Link
2024-05-01	[anatomage.com]	lockbit3	Link
2024-05-01	[bluegrasstechnologies.net]	lockbit3	Link
2024-05-01	[PINNACLEENGR.COM]	clop	Link
2024-05-01	[MCKINLEYPACKAGING.COM]	clop	Link
2024-05-01	[PILOTPEN.COM]	clop	Link
2024-05-01	[colonial.edu]	lockbit3	Link
2024-05-01	[cordish.com]	lockbit3	Link
2024-05-01	[concorr.com]	lockbit3	Link
2024-05-01	[yupousa.com]	lockbit3	Link
2024-05-01	[peaseinc.com]	lockbit3	Link
2024-05-01	[bdcm.com]	blackbasta	Link
2024-05-01	[MORTON WILLIAMS]	everest	Link
2024-05-03	[melting-mind.de]	apt73	Link
2024-05-21	[netscout.com]	dispossessor	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.