Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240502

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

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

—

Jetzt patchen! Attacken auf Dateiübertragungsserver CrushFTP beobachtet

Angreifer haben Zugriff auf Systemdaten von CrushFTP-Servern. Verwundbare Systeme gibt es auch in Deutschland.

- Link

—

FIDO2-Sticks: Lücke in Yubikey-Verwaltungssoftware erlaubt Rechteausweitung

Um die FIDO2-Sticks von Yubikey zu verwalten, stellt der Hersteller eine Software bereit. Eine Lücke darin ermöglicht die Ausweitung der Rechte.

- Link

—

Mitel SIP-Phones anfällig für unbefugte Zugriffe

Mitel-SIP-Phones und -Konferenz-Produkte ermöglichen unbefugte Zugriffe und das Ausführen von Schadcode. Updates stehen bereit.

- Link

—

Update für Solarwinds FTP-Server Serv-U schließt Lücke mit hohem Risiko

Im Solarwinds Serv-U-FTP-Server klafft eine als hohes Risiko eingestufte Sicherheitslücke. Der Hersteller dichtet sie mit einem Update ab.

- 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-2023-6895	0.901600000	0.987640000	Link
CVE-2023-6553	0.916210000	0.988720000	Link
CVE-2023-5360	0.967230000	0.996480000	Link
CVE-2023-4966	0.966100000	0.996160000	Link
CVE-2023-49103	0.901710000	0.987660000	Link
CVE-2023-48795	0.962250000	0.995020000	Link
CVE-2023-47246	0.941130000	0.991350000	Link
CVE-2023-46805	0.965580000	0.996020000	Link
CVE-2023-46747	0.971350000	0.997930000	Link
CVE-2023-46604	0.972480000	0.998390000	Link
CVE-2023-43177	0.964020000	0.995530000	Link
CVE-2023-42793	0.971040000	0.997740000	Link
CVE-2023-39143	0.950730000	0.992960000	Link
CVE-2023-38646	0.913020000	0.988480000	Link
CVE-2023-38203	0.972020000	0.998180000	Link
CVE-2023-38035	0.973610000	0.998950000	Link
CVE-2023-36845	0.965540000	0.996020000	Link
CVE-2023-3519	0.911860000	0.988420000	Link
CVE-2023-35082	0.952190000	0.993170000	Link
CVE-2023-35078	0.966030000	0.996130000	Link
CVE-2023-34993	0.956820000	0.993960000	Link
CVE-2023-34960	0.938540000	0.991060000	Link
CVE-2023-34634	0.918830000	0.988960000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34362	0.955450000	0.993710000	Link
CVE-2023-34039	0.934640000	0.990580000	Link
CVE-2023-3368	0.918440000	0.988940000	Link
CVE-2023-33246	0.973120000	0.998690000	Link
CVE-2023-32315	0.974090000	0.999260000	Link
CVE-2023-32235	0.911650000	0.988390000	Link
CVE-2023-30625	0.945200000	0.992100000	Link
CVE-2023-30013	0.960350000	0.994610000	Link
CVE-2023-29300	0.970030000	0.997350000	Link
CVE-2023-29298	0.948030000	0.992480000	Link
CVE-2023-28771	0.914030000	0.988550000	Link
CVE-2023-28432	0.940320000	0.991260000	Link
CVE-2023-28121	0.945870000	0.992180000	Link
CVE-2023-27524	0.970430000	0.997500000	Link
CVE-2023-27372	0.973780000	0.999030000	Link
CVE-2023-27350	0.970720000	0.997620000	Link
CVE-2023-26469	0.933870000	0.990500000	Link
CVE-2023-26360	0.964040000	0.995540000	Link
CVE-2023-26035	0.969280000	0.997100000	Link
CVE-2023-25717	0.957880000	0.994160000	Link
CVE-2023-25194	0.969190000	0.997080000	Link
CVE-2023-2479	0.963600000	0.995400000	Link
CVE-2023-24489	0.974290000	0.999390000	Link
CVE-2023-23752	0.932080000	0.990300000	Link
CVE-2023-23397	0.926450000	0.989810000	Link
CVE-2023-23333	0.963260000	0.995300000	Link
CVE-2023-22527	0.974440000	0.999460000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-22518	0.966340000	0.996220000	Link
CVE-2023-22515	0.972060000	0.998180000	Link
CVE-2023-21839	0.958250000	0.994220000	Link
CVE-2023-21554	0.959160000	0.994390000	Link
CVE-2023-20887	0.961910000	0.994960000	Link
CVE-2023-1671	0.967280000	0.996520000	Link
CVE-2023-0669	0.969750000	0.997250000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 30 Apr 2024

[UPDATE] [hoch] X.Org X11: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in X.Org X11 ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Tue, 30 Apr 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um vertrauliche Informationen offenzulegen oder einen nicht näher spezifizierten Angriff zu starten.

- Link

—

Tue, 30 Apr 2024

[UPDATE] [hoch] X.Org X11: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in X.Org X11 ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Tue, 30 Apr 2024

[UPDATE] [hoch] GNU Emacs: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in GNU Emacs ausnutzen, um beliebigen Programmcode auszuführen oder Sicherheitsvorkehrungen zu umgehen.
- Link

—

Tue, 30 Apr 2024

[NEU] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder seine Privilegien zu erweitern.
- Link

—

Tue, 30 Apr 2024

[NEU] [hoch] Acronis Cyber Protect: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Acronis Cyber Protect ausnutzen, um Informationen offenzulegen, sensible Daten zu ändern und um seine Berechtigungen zu erhöhen.
- Link

—

Tue, 30 Apr 2024

[UPDATE] [hoch] FRRouting Project FRRouting: Mehrere Schwachstellen ermöglichen Denial of Service

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in FRRouting Project FRRouting ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

Tue, 30 Apr 2024

[UPDATE] [hoch] libsndfile: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in libsndfile ausnutzen, um beliebigen Code auszuführen, einen ‘Denial of Service’-Zustand herbeizuführen oder einen nicht spezifizierten Angriff durchzuführen.
- Link

—

Tue, 30 Apr 2024

[UPDATE] [hoch] GStreamer: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in GStreamer ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Tue, 30 Apr 2024

[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Tue, 30 Apr 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

—

Tue, 30 Apr 2024

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

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

- Link

—

Tue, 30 Apr 2024

[UPDATE] [hoch] EDK2 NetworkPkg IP stack implementation: Mehrere Schwachstellen

Ein Angreifer aus dem angrenzenden Netzwerk oder ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der EDK2 NetworkPkg IP stack implementation ausnutzen, um beliebigen Programmcode auszuführen, vertrauliche Informationen offenzulegen und einen Denial of Service Zustand auszulösen.

- Link

—

Tue, 30 Apr 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

—

Tue, 30 Apr 2024

[UPDATE] [hoch] Red Hat Ansible Automation Platform: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat Ansible Automation Platform ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren, Phishing-Angriffe durchzuführen oder Cross-Site Scripting (XSS)-Angriffe auszuführen. Einige dieser Schwachstellen erfordern eine Benutzerinteraktion, um sie erfolgreich auszunutzen.

- Link

—

Tue, 30 Apr 2024

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

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

- Link

—

Tue, 30 Apr 2024

[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen und weitere, nicht spezifizierte Auswirkungen zu verursachen.

- Link

—

Tue, 30 Apr 2024

[NEU] [UNGEPATCHT] [hoch] D-LINK Router: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in D-LINK Router ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Tue, 30 Apr 2024

[NEU] [hoch] Extreme Networks ExtremeXOS: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Extreme Networks ExtremeXOS ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Tue, 30 Apr 2024

[UPDATE] [hoch] Grub2: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein Angreifer kann mehrere Schwachstellen in Oracle Linux ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
5/1/2024	[Debian dla-3805 : libqt5concurrent5 - security update]	critical
5/1/2024	[SUSE SLES15 Security Update : python311 (SUSE-SU-2024:0782-2)]	critical
5/1/2024	[RHEL 8 / 9 : Red Hat Ceph Storage 6.1 (RHSA-2024:2631)]	critical
5/1/2024	[Fedora 40 : tpm2-tools / tpm2-tss (2024-0c9d3b51d4)]	critical
5/1/2024	[CentOS 7 : rhc-worker-script (RHSA-2024:2625)]	high
5/1/2024	[SUSE SLES15 Security Update : frr (SUSE-SU-2024:1475-1)]	high
5/1/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2024:1480-1)]	high
5/1/2024	[RHEL 9 : kernel (RHSA-2024:2627)]	high
5/1/2024	[IBM MQ DoS (7123139)]	high
5/1/2024	[Debian dla-3806 : distro-info-data - security update]	high
5/1/2024	[RHEL 9 : podman (RHSA-2024:2645)]	high
5/1/2024	[Fedora 38 : thunderbird (2024-15b892ebd3)]	high
5/1/2024	[Fedora 39 : et (2024-94a155818c)]	high
5/1/2024	[Fedora 38 : et (2024-bd9e67c117)]	high
5/1/2024	[Fedora 40 : et (2024-b745c97f4b)]	high
5/1/2024	[Fedora 40 : php-tcpdf (2024-27eafd0e65)]	high
4/30/2024	[Amazon Linux 2 : qt5-qtbase (ALAS-2024-2533)]	high
4/30/2024	[Amazon Linux 2 : glibc (ALAS-2024-2521)]	high
4/30/2024	[Amazon Linux 2 : wireshark (ALAS-2024-2522)]	high
4/30/2024	[Amazon Linux 2 : jose (ALAS-2024-2529)]	high
4/30/2024	[Amazon Linux 2 : httpd (ALAS-2024-2532)]	high
4/30/2024	[Amazon Linux 2 : bind (ALAS-2024-2530)]	high
4/30/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.10-2024-054)]	high
4/30/2024	[Amazon Linux 2 : libreoffice (ALASLIBREOFFICE-2024-003)]	high

Datum	Schwachstelle	Bewertung
4/30/2024	[Amazon Linux 2 : mod_http2 (ALAS-2024-2524)]	high
4/30/2024	[Amazon Linux 2 : firefox (ALASFIREFOX-2024-024)]	high
4/30/2024	[RHEL 8 : container-tools:rhel8 (RHSA-2024:2090)]	high
4/30/2024	[RHEL 9 : podman (RHSA-2024:2089)]	high
4/30/2024	[RHEL 9 : kernel-rt (RHSA-2024:2628)]	high
4/30/2024	[RHEL 7 : rhc-worker-script (RHSA-2024:2625)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“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

—

” “Tue, 23 Apr 2024

Palo Alto PAN-OS Command Execution / Arbitrary File Creation

Palo Alto PAN-OS versions prior to 11.1.2-h3 command injection and arbitrary file creation exploit.
- Link

—

” “Mon, 22 Apr 2024

LRMS PHP 1.0 SQL Injection / Shell Upload

LRMS PHP version 1.0 suffers from remote shell upload and multiple remote SQL injection vulnerabilities.
- Link

—

” “Mon, 22 Apr 2024

Dreamehome 2.1.5 Broken Authorization

Dreamehome versions 2.1.5 and below suffer from multiple broken authorization vulnerabilities.
- Link

—

” “Mon, 22 Apr 2024

SofaWiki 3.9.2 Shell Upload

SofaWiki version 3.9.2 suffers from a remote shell upload vulnerability.
- Link

—

” “Mon, 22 Apr 2024

Laravel Framework 11 Credential Disclosure

Laravel Framework version 11 suffers from a credential disclosure vulnerability.
- Link

—

” “Fri, 19 Apr 2024

FlatPress 1.3 Shell Upload

FlatPress version 1.3 suffers from a remote shell upload vulnerability.
- Link

—

” “Fri, 19 Apr 2024

MindManager Local Privilege Escalation

MindManager suffers from a local privilege escalation vulnerability via MSI installer Repair Mode.
- Link

—

”

4.2 0-Days der letzten 5 Tage

“Wed, 01 May 2024

ZDI-24-419: (Pwn2Own) Xiaomi Pro 13 GetApps integral-dialog-page Cross-Site Scripting Remote Code Execution Vulnerability

- Link

—

” “Wed, 01 May 2024

ZDI-24-418: (Pwn2Own) Xiaomi Pro 13 mimarket manual-upgrade Cross-Site Scripting Remote Code Execution Vulnerability

- Link

—

” “Wed, 01 May 2024

ZDI-24-417: Xiaomi Pro 13 isUrlMatchLevel Permissive List of Allowed Inputs Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Apr 2024

ZDI-24-416: Centreon sysName Cross-Site Scripting Remote Code Execution Vulnerability

- Link

—

”

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

7 Ransomware-Erpressungen: (Mai)

Datum	Opfer	Ransomware-Grupppe	Webseite
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.