Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241202

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

ProFTPD: Angreifer können Rechte ausweiten

In ProFTPD können Angreifer eine Sicherheitslücke missbrauchen, um ihre Rechte im System auszuweiten. Quellcode-Updates stehen bereit.

- Link

—

Jetzt patchen! Attacken auf Filesharingplattform ProjectSend beobachtet

Auch wenn ein Sicherheitspatch für ProjectSend schon länger als ein Jahr verfügbar ist, sind offensichtlich noch unzählige Instanzen verwundbar.

- Link

—

Hochriskante Sicherheitslücke in PostgreSQL: Gitlab patcht (noch) nicht

Eine bekannte Lücke ermöglicht es einfachen Nutzern, in PostgreSQL Befehle einzuschleusen. Ein Update gäbe es. GitLab installiert es bislang nicht.

- Link

—

Sicherheitslecks in Entwicklerwerkzeug Jenkins gestopft

In dem Software-Entwicklungs-Tool Jenkins haben die Entwickler mehrere Sicherheitslücken gefunden. Updates schließen sie.

- Link

—

Manageengine Analytics Plus: Sicherheitslücke erlaubt Rechteausweitung

In Zohocorps Manageengine Analytics Plus können Angreifer eine Sicherheitslücke missbrauchen, um ihre Rechte auszuweiten.

- Link

—

Sicherheitsupdates: Vielfältige Angriffe auf Synology NAS und BeeDrive möglich

Synology hat unter anderem mehrere Schwachstellen im NAS-Betriebssystem DSM und der Backupsoftware BeeDrive geschlossen.

- Link

—

Palo Alto Globalprotect: Schadcode-Lücke durch unzureichende Zertifikatsprüfung

Eine Sicherheitslücke in Palo Alto Networks Globalprotect-VPN-App ermöglicht Angreifern, Rechner vollständig zu kompromittieren.

- Link

—

Microsoft patcht teils kritische Lücken außer der Reihe

Microsoft hat Sicherheitslecks in mehreren Produkten geschlossen. Einige Updates müssen Nutzer installieren.

- Link

—

Root-Sicherheitslücken in VMware Aria Operations geschlossen

VMwares IT-Verwaltungsplattform Aria Operations ist verwundbar. Admins sollten die Sicherheitspatches in Bälde installieren.

- Link

—

HPE Insight Remote Support: Monitoring-Software ermöglicht Codeschmuggel

In der kostenlosen Monitoring-Software HPE Insight Remote Support ermöglichen teils kritische Sicherheitslücken das Einschleusen von Schadcode.

- 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	0.955020000	0.994650000	Link
CVE-2023-6895	0.936280000	0.992190000	Link
CVE-2023-6553	0.952340000	0.994240000	Link
CVE-2023-6019	0.935090000	0.992050000	Link
CVE-2023-6018	0.916750000	0.990350000	Link
CVE-2023-52251	0.947690000	0.993540000	Link
CVE-2023-4966	0.971030000	0.998310000	Link
CVE-2023-49103	0.948250000	0.993630000	Link
CVE-2023-48795	0.962800000	0.995960000	Link
CVE-2023-47246	0.963300000	0.996080000	Link
CVE-2023-46805	0.959100000	0.995310000	Link
CVE-2023-46747	0.972680000	0.998930000	Link
CVE-2023-46604	0.967810000	0.997320000	Link
CVE-2023-4542	0.941060000	0.992710000	Link
CVE-2023-43208	0.974210000	0.999550000	Link
CVE-2023-43177	0.959840000	0.995440000	Link
CVE-2023-42793	0.971260000	0.998390000	Link
CVE-2023-41265	0.912600000	0.990120000	Link
CVE-2023-39143	0.920260000	0.990640000	Link
CVE-2023-38205	0.953810000	0.994450000	Link
CVE-2023-38203	0.964750000	0.996410000	Link
CVE-2023-38146	0.906640000	0.989670000	Link
CVE-2023-38035	0.974360000	0.999610000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.967890000	0.997340000	Link
CVE-2023-3519	0.965540000	0.996640000	Link
CVE-2023-35082	0.963840000	0.996210000	Link
CVE-2023-35078	0.967840000	0.997330000	Link
CVE-2023-34993	0.972760000	0.998970000	Link
CVE-2023-34634	0.926130000	0.991090000	Link
CVE-2023-34362	0.970200000	0.998050000	Link
CVE-2023-34039	0.929610000	0.991470000	Link
CVE-2023-3368	0.937890000	0.992340000	Link
CVE-2023-33246	0.973040000	0.999030000	Link
CVE-2023-32315	0.973370000	0.999170000	Link
CVE-2023-32235	0.914280000	0.990230000	Link
CVE-2023-30625	0.950240000	0.993890000	Link
CVE-2023-30013	0.968110000	0.997390000	Link
CVE-2023-29300	0.968250000	0.997440000	Link
CVE-2023-29298	0.969330000	0.997720000	Link
CVE-2023-28432	0.906870000	0.989680000	Link
CVE-2023-28343	0.966250000	0.996810000	Link
CVE-2023-28121	0.929810000	0.991490000	Link
CVE-2023-27524	0.970390000	0.998100000	Link
CVE-2023-27372	0.973870000	0.999390000	Link
CVE-2023-27350	0.968620000	0.997520000	Link
CVE-2023-26469	0.957610000	0.995080000	Link
CVE-2023-26360	0.962010000	0.995820000	Link
CVE-2023-26035	0.968960000	0.997600000	Link
CVE-2023-25717	0.949440000	0.993770000	Link
CVE-2023-25194	0.967670000	0.997290000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963800000	0.996190000	Link
CVE-2023-24489	0.972870000	0.998990000	Link
CVE-2023-23752	0.948310000	0.993630000	Link
CVE-2023-23397	0.902750000	0.989420000	Link
CVE-2023-23333	0.963300000	0.996080000	Link
CVE-2023-22527	0.969680000	0.997840000	Link
CVE-2023-22518	0.963120000	0.996040000	Link
CVE-2023-22515	0.973360000	0.999160000	Link
CVE-2023-21839	0.933960000	0.991930000	Link
CVE-2023-21554	0.951950000	0.994140000	Link
CVE-2023-20887	0.968860000	0.997580000	Link
CVE-2023-1698	0.911050000	0.990030000	Link
CVE-2023-1671	0.962610000	0.995900000	Link
CVE-2023-0669	0.972180000	0.998740000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 29 Nov 2024

[UPDATE] [hoch] Fortinet FortiClient: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Fortinet FortiClient ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 29 Nov 2024

[UPDATE] [hoch] Fortinet FortiClient: Mehrere Schwachstellen ermöglichen Codeausführung

Ein lokaler Angreifer kann mehrere Schwachstellen in Fortinet FortiClient ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 29 Nov 2024

[UPDATE] [hoch] Fortinet FortiOS: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Fortinet FortiOS und Fortinet FortiProxy ausnutzen, um Informationen offenzulegen.

- Link

—

Fri, 29 Nov 2024

[UPDATE] [hoch] TIBCO JasperReports: Mehrere Schwachstellen

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in TIBCO JasperReports ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder Cross-Site Scripting (XSS)-Angriffe durchzuführen.

- Link

—

Fri, 29 Nov 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

—

Fri, 29 Nov 2024

[UPDATE] [hoch] Internet Systems Consortium BIND: Mehrere Schwachstellen ermöglichen Denial of Service

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Internet Systems Consortium BIND ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Fri, 29 Nov 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Logback ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Fri, 29 Nov 2024

[UPDATE] [hoch] Node.js: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder seine

Privilegien zu erweitern.
- Link

—

Fri, 29 Nov 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

—

Fri, 29 Nov 2024

[UPDATE] [hoch] Redis: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Redis ausnutzen, um einen Denial of Service Angriff durchzuführen oder Code auszuführen.
- Link

—

Fri, 29 Nov 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

—

Fri, 29 Nov 2024

[UPDATE] [hoch] PostgreSQL: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, Daten zu manipulieren oder vertrauliche Informationen preiszugeben.
- Link

—

Fri, 29 Nov 2024

[UPDATE] [hoch] cobbler: Schwachstelle ermöglicht Erlangen von Administratorrechten

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in cobbler ausnutzen, um Administratorrechte zu erlangen.
- Link

—

Fri, 29 Nov 2024

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PHP ausnutzen, um vertrauliche Informationen preiszugeben, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu

erzeugen und einen Spoofing-Angriff durchzuführen.

- Link

—

Fri, 29 Nov 2024

[UPDATE] [hoch] Mozilla Firefox und 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 preiszugeben, Sicherheitsmaßnahmen zu umgehen oder Cross-Site-Scripting- oder Spoofing-Angriffe durchzuführen.

- Link

—

Fri, 29 Nov 2024

[UPDATE] [hoch] WebKit: Mehrere Schwachstellen ermöglichen Cross-Site Scripting und und Code-Ausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in WebKit ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen und beliebigen Code auszuführen.

- Link

—

Fri, 29 Nov 2024

[UPDATE] [hoch] Zyxel Firewall: Schwachstelle ermöglicht Manipulation von Dateien

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Zyxel Firewall ausnutzen, um Dateien zu manipulieren.

- Link

—

Fri, 29 Nov 2024

[NEU] [hoch] ProFTPD: Schwachstelle ermöglicht Privilegieneskalation

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

- Link

—

Thu, 28 Nov 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

—

Thu, 28 Nov 2024

[UPDATE] [hoch] Apache CloudStack: Mehrere Schwachstellen ermöglichen Privilegieneskalation
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache CloudStack ausnutzen, um die Authentifizierung zu umgehen, vertrauliche Informationen offenzulegen oder seine Privilegien zu erweitern und so die Kontrolle über das System zu übernehmen.
- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
11/29/2024	[Fedora 41 : rust-rustls / rust-zlib-rs (2024-41e6e2fc74)]	critical
11/29/2024	[Fedora 41 : thunderbird (2024-07f6b6766c)]	critical
11/29/2024	[Fedora 40 : rust-rustls / rust-zlib-rs (2024-632b468c59)]	critical
11/29/2024	[Fedora 41 : firefox / nss (2024-b266d38c44)]	critical
11/29/2024	[Debian dla-3975 : proftpd-basic - security update]	critical
11/29/2024	[Phoenix Contact Classic Line Industrial Controllers Missing Authentication For Critical Function (CVE-2019-9201)]	critical
11/29/2024	[Axis Communication Network Cameras and Video Servers Unauthenticated Device Administration (CVE-2004-2427)]	critical
12/1/2024	[Fedora 40 : wireshark (2024-0b563ad294)]	high
12/1/2024	[Fedora 40 : qbittorrent (2024-ab5ad835c1)]	high
12/1/2024	[Fedora 41 : wireshark (2024-f9f740bc60)]	high
12/1/2024	[Fedora 41 : webkitgtk (2024-472d01833c)]	high
11/30/2024	[Debian dla-3974 : dnsmasq - security update]	high
11/29/2024	[Fedora 41 : tuned (2024-e457d67157)]	high
11/29/2024	[Fedora 41 : pam (2024-4d4d946073)]	high
11/29/2024	[Cisco (CVE-2020-3398)]	high
11/29/2024	[Cisco (CVE-2020-3338)]	high

Datum	Schwachstelle	Bewertung
11/29/2024	[Cisco (CVE-2020-3397)]	high
11/29/2024	[Cisco (CVE-2020-3394)]	high
11/29/2024	[Dell UPnP SUBSCRIBE function Incorrect Default Permissions (CVE-2020-12695)]	high
11/29/2024	[Cisco Nexus Uncontrolled Resource Consumption (CVE-2020-3168)]	high
11/29/2024	[Phoenix Contact PLC Cycle Time Influences Uncontrolled Resource Consumption (CVE-2019-10953)]	high
11/29/2024	[Eaton 9PX Cross-Site Request Forgery (CVE-2018-9281)]	high
11/29/2024	[Cisco NX-OS Improper Input Validation (CVE-2018-0456)]	high
11/29/2024	[Axis Communication Network Cameras and Video Servers Arbitrary OS Commands Execution (CVE-2004-2425)]	high
11/28/2024	[Debian dla-3969 : thunderbird - security update]	high
11/28/2024	[Intel Neural Compressor < 3.0 Multiple Vulnerabilities]	high
11/28/2024	[Cisco IOS XE Software Web UI XSRF (cisco-sa-webui-csrf-ycUYxkKO)]	high
11/28/2024	[Debian dla-3971 : firefox-esr - security update]	high
11/28/2024	[Debian dla-3972 : tzdata - security update]	high
11/28/2024	[Oracle Linux 7 : java-11-openjdk (ELSA-2024-8120)]	high
11/28/2024	[Oracle Linux 7 : java-1.8.0-openjdk (ELSA-2024-8116)]	high
11/28/2024	[Schneider Electric Modicon M340, MC80, and Momentum Unity M1E Arbitrary Code Execution (CVE-2024-8938)]	high
11/28/2024	[Schneider Electric Modicon M340, MC80, and Momentum Unity M1E Authentication Bypass by Spoofing (CVE-2024-8935)]	high
11/28/2024	[Schneider Electric Modicon M340, MC80, and Momentum Unity M1E Denial of Service (CVE-2024-8933)]	high
11/28/2024	[Cisco (CVE-2020-3454)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Wed, 27 Nov 2024

ABB Cylon Aspect 3.08.01 vstatConfigurationDownload.php Configuration Download

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated configuration download vulnerability. This can be exploited to download the CSV DB that contains the configuration mappings information via the VMobileImportExportServlet by directly calling the vstatConfigurationDownload.php script.

- Link

—

” “Wed, 27 Nov 2024

Akuvox Smart Intercom/Doorphone ServicesHTTPAPI Improper Access Control

The Akuvox Smart Intercom/Doorphone suffers from an insecure service API access control. The vulnerability in ServicesHTTPAPI endpoint allows users with ”User” privileges to modify API access settings and configurations. This improper access control permits privilege escalation, enabling unauthorized access to administrative functionalities. Exploitation of this issue could compromise system integrity and lead to unauthorized system modifications.

- Link

—

” “Fri, 22 Nov 2024

CUPS IPP Attributes LAN Remote Code Execution

This Metasploit module exploits vulnerabilities in OpenPrinting CUPS, which is running by default on most Linux distributions. The vulnerabilities allow an attacker on the LAN to advertise a malicious printer that triggers remote code execution when a victim sends a print job to the malicious printer. Successful exploitation requires user interaction, but no CUPS services need to be reachable via accessible ports. Code execution occurs in the context of the lp user. Affected versions are cups-browsed less than or equal to 2.0.1, libcupsfilters versions 2.1b1 and below, libppd versions 2.1b1 and below, and cups-filters versions 2.0.1 and below.

- Link

—

” “Fri, 22 Nov 2024

ProjectSend R1605 Unauthenticated Remote Code Execution

This Metasploit module exploits an improper authorization vulnerability in ProjectSend versions r1295 through r1605. The vulnerability allows an unauthenticated attacker to obtain remote code execution by enabling user registration, disabling the whitelist of allowed file extensions, and uploading a malicious PHP file to the server.

- Link

—

” “Fri, 22 Nov 2024

needrestart Local Privilege Escalation

Qualys discovered that needrestart suffers from multiple local privilege escalation vulnerabilities that allow for root access from an unprivileged user.

- Link

—

” “Fri, 22 Nov 2024

fronsetia 1.1 Cross Site Scripting

fronsetia version 1.1 suffers from a cross site scripting vulnerability.

- Link

—

” “Fri, 22 Nov 2024

fronsetia 1.1 XML Injection

fronsetia version 1.1 suffers from an XML external entity injection vulnerability.

- Link

—

” “Fri, 22 Nov 2024

PowerVR psProcessHandleBase Reuse

PowerVR has an issue where PVRSRVAcquireProcessHandleBase() can cause psProcessHandleBase reuse when PIDs are reused.

- Link

—

” “Fri, 22 Nov 2024

Linux 6.6 Race Condition

A security-relevant race between mremap() and THP code has been discovered. Reaching the buggy code typically requires the ability to create unprivileged namespaces. The bug leads to installing physical address 0 as a page table, which is likely exploitable in several ways: For example, triggering the bug in multiple processes can probably lead to unintended page table sharing, which probably can lead to stale TLB entries pointing to freed pages.

- Link

—

” “Fri, 22 Nov 2024

Korenix JetPort 5601 1.2 Path Traversal

Korenix JetPort 5601 version 1.2 suffers from a path traversal vulnerability.

- Link

—

” “Fri, 22 Nov 2024

SEH utnserver Pro 20.1.22 Cross Site Scripting

SEH utnservyer Pro version 20.1.22 suffers from multiple persistent cross site scripting vulnerabilities.

- Link

—

” “Thu, 21 Nov 2024

Ivanti EPM Agent Portal Command Execution

This Metasploit module leverages an unauthenticated remote command execution vulnerability in Ivanti’s EPM Agent Portal where an RPC client can invoke a method which will run an attacker-specified string on the remote target as NT AUTHORITY\SYSTEM. This vulnerability is present in versions prior to EPM 2021.1 Su4 and EPM 2022 Su2.

- Link

—

” “Thu, 21 Nov 2024

Judge0 Sandbox Escape

Judge0 does not account for symlinks placed inside the sandbox directory, which can be leveraged by an attacker to write to arbitrary files and gain code execution outside of the sandbox.

- Link

—

” “Tue, 19 Nov 2024

WordPress Really Simple Security Authentication Bypass

WordPress Really Simple Security plugin versions prior to 9.1.2 proof of concept authentication bypass exploit.

- Link

—

” “Tue, 19 Nov 2024

Palo Alto PAN-OS Authentication Bypass / Remote Command Execution

Proof of concept code to exploit an authentication bypass in Palo Alto’s PAN-OS that is coupled with remote command execution.

- Link

—

” “Mon, 18 Nov 2024

Pyload Remote Code Execution

CVE-2024-28397 is a sandbox escape in js2py versions 0.74 and below. js2py is a popular python package that can evaluate javascript code inside a python interpreter. The vulnerability allows for an attacker to obtain a reference to a python object in the js2py environment enabling them to escape the sandbox, bypass pyimport restrictions and execute arbitrary commands on the host. At the time of this writing no patch has been released and version 0.74 is the latest version of js2py

which was released Nov 6, 2022. CVE-2024-39205 is a remote code execution vulnerability in Pyload versions 0.5.0b3.dev85 and below. It is an open-source download manager designed to automate file downloads from various online sources. Pyload is vulnerable because it exposes the vulnerable js2py functionality mentioned above on the /flash/addcrypted2 API endpoint. This endpoint was designed to only accept connections from localhost but by manipulating the HOST header we can bypass this restriction in order to access the API to achieve unauthenticated remote code execution.

- Link

—

” “Mon, 18 Nov 2024

SOPlanning 1.52.01 Remote Code Execution

SOPlanning version 1.52.01 authenticated remote code execution exploit.

- Link

—

” “Thu, 14 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

—

” “Thu, 14 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

—

” “Thu, 14 Nov 2024

GravCMS 1.10.7 Arbitrary YAML Write / Update

Proof of concept remote code execution exploit for GravCMS 1.10.7 that leverages an arbitrary YAML write / update.

- Link

—

” “Thu, 14 Nov 2024

PHP-CGI Argument Injection Remote Code Execution

Proof of concept remote code execution exploit for PHP-CGI that affects versions 8.1 before 8.1.29, 8.2 before 8.2.20, and 8.3 before 8.3.8.

- 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

—

”

4.2 0-Days der letzten 5 Tage

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Gehackt via Nachbar... oder die Palo Alto.

Zum Youtube Video

6 Cyberangriffe: (Dez)

Datum	Opfer	Land	Information

7 Ransomware-Erpressungen: (Dez)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-12-01	[shapesmfg.com]	ransomhub	Link
2024-12-01	[everde.com]	ransomhub	Link
2024-12-01	[qualitybillingservice.com]	ransomhub	Link
2024-12-01	[tascosaofficemachines.com]	ransomhub	Link
2024-12-01	[costelloeye.com]	ransomhub	Link
2024-12-01	[McKibbin]	incransom	Link
2024-12-01	[Alpine Ear Nose & Throat]	bianlian	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.