Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240604

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

Sicherheitsupdate: Schadcode-Attacken auf Autodesk AutoCAD möglich
Die CAD-Softwares Advance Steel, Civil 3D und AutoCAD von Autodesk sind verwundbar. Das Sicherheitsrisiko gilt als hoch.
- Link

—

Linux: root-Lücke wird aktiv missbraucht
Die IT-Sicherheitsbehörde CISA warnt vor aktiven Angriffen auf eine Linux-Lücke. Angreifer verschaffen sich damit root-Rechte.
- Link

—

IT-Monitoring: Checkmk schließt Lücke, die Änderung von Dateien ermöglicht
Eine Sicherheitslücke in der Monitoring-Software Checkmk ermöglicht Angreifern, unbefugt lokale Dateien auf dem Checkmk-Server zu lesen und zu schreiben.
- Link

—

Notfallpatch: Angreifer attackieren VPN-Verbindungen von Checkpoint Gateways
Checkpoint hat ein Notfall-Sicherheitsupdate veröffentlicht. Derzeit haben Angreifer Network Security Gateways wie Quantum Maestro im Visier.
- Link

—

Foxit PDF Reader: Halbherzige Zertifikatprüfung ermöglicht Rechteausweitung
Die Update-Routinen vom Foxit PDF Reader prüfen Zertifikate nicht richtig. Angreifer können dadurch ihre Rechte ausweiten.
- Link

—

Proof-of-Concept-Exploits für kritische FortiSIEM-Lücken: Jetzt patchen!
IT-Sicherheitsforscher haben für kritische Sicherheitslücken in FortiSIEM Proof-of-Concept-Exploits veröffentlicht. Höchste Zeit, die Updates zu installieren.
- Link

—

Supportende: Rechte-Sicherheitslücke gefährdet Ivanti Endpoint Manager 2021
Angreifer können Schadcode mit erhöhten Rechten ausführen. Admins müssen Ivanti EPM auf eine noch unterstützte Version upgraden.
- Link

—

Kritische Sicherheitslücke gewährt Angreifern Zugriff auf TP-Link-Router C5400X

Der TP-Link-WLAN-Router C5400X ist verwundbar. Ein Sicherheitspatch schließt eine kritische Schwachstelle.

- Link

—

Windows Server 2019: Aktualisiertes Sicherheitsupdate behebt Installationsfehler

Das Sicherheitsupdate für Windows Server 2019 schlug mit den Fehlernummern 0x800f0982 und 0x80004005 fehl. Ein aktualisiertes Update ist verfügbar.

- Link

—

GitLab: Accountübernahme nach 1-Klick-Attacke möglich

Mehrere Sicherheitslücken in GitLab gefährden Systeme. Gegen mögliche Attacken gerüstete Versionen stehen zum Download bereit.

- 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	0.959520000	0.994660000	Link
CVE-2023-6553	0.923550000	0.989590000	Link
CVE-2023-5360	0.965120000	0.995980000	Link
CVE-2023-4966	0.969890000	0.997390000	Link
CVE-2023-48795	0.959010000	0.994560000	Link
CVE-2023-47246	0.935450000	0.990940000	Link
CVE-2023-46805	0.963760000	0.995640000	Link
CVE-2023-46747	0.971460000	0.998040000	Link
CVE-2023-46604	0.922790000	0.989500000	Link
CVE-2023-4542	0.922430000	0.989450000	Link
CVE-2023-43208	0.963060000	0.995430000	Link
CVE-2023-43177	0.960230000	0.994820000	Link
CVE-2023-42793	0.970430000	0.997600000	Link
CVE-2023-41265	0.914120000	0.988820000	Link
CVE-2023-39143	0.948440000	0.992800000	Link
CVE-2023-38646	0.908390000	0.988370000	Link
CVE-2023-38205	0.928030000	0.990140000	Link
CVE-2023-38203	0.970370000	0.997570000	Link
CVE-2023-38146	0.905210000	0.988140000	Link
CVE-2023-38035	0.975060000	0.999840000	Link
CVE-2023-36845	0.966630000	0.996380000	Link
CVE-2023-3519	0.911860000	0.988670000	Link
CVE-2023-35082	0.968540000	0.997000000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-35078	0.968250000	0.996920000	Link
CVE-2023-34993	0.967190000	0.996540000	Link
CVE-2023-34960	0.933660000	0.990760000	Link
CVE-2023-34634	0.923550000	0.989600000	Link
CVE-2023-34362	0.961530000	0.995050000	Link
CVE-2023-34039	0.944630000	0.992170000	Link
CVE-2023-3368	0.932830000	0.990690000	Link
CVE-2023-33246	0.972320000	0.998400000	Link
CVE-2023-32315	0.973460000	0.998940000	Link
CVE-2023-32235	0.914550000	0.988840000	Link
CVE-2023-30625	0.950680000	0.993150000	Link
CVE-2023-30013	0.963050000	0.995430000	Link
CVE-2023-29300	0.969710000	0.997350000	Link
CVE-2023-29298	0.942510000	0.991760000	Link
CVE-2023-28771	0.918640000	0.989190000	Link
CVE-2023-28121	0.932700000	0.990670000	Link
CVE-2023-27524	0.971240000	0.997970000	Link
CVE-2023-27372	0.973760000	0.999070000	Link
CVE-2023-27350	0.971140000	0.997910000	Link
CVE-2023-26469	0.942400000	0.991750000	Link
CVE-2023-26360	0.952190000	0.993420000	Link
CVE-2023-26035	0.967700000	0.996760000	Link
CVE-2023-25717	0.956860000	0.994190000	Link
CVE-2023-25194	0.968000000	0.996850000	Link
CVE-2023-2479	0.963670000	0.995620000	Link
CVE-2023-24489	0.973760000	0.999070000	Link
CVE-2023-23752	0.932080000	0.990580000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23397	0.922480000	0.989460000	Link
CVE-2023-23333	0.963260000	0.995490000	Link
CVE-2023-22527	0.974590000	0.999580000	Link
CVE-2023-22518	0.962670000	0.995310000	Link
CVE-2023-22515	0.973130000	0.998750000	Link
CVE-2023-21839	0.959090000	0.994580000	Link
CVE-2023-21554	0.955760000	0.994010000	Link
CVE-2023-20887	0.965950000	0.996220000	Link
CVE-2023-20198	0.915340000	0.988930000	Link
CVE-2023-1698	0.912990000	0.988720000	Link
CVE-2023-1671	0.969090000	0.997140000	Link
CVE-2023-0669	0.969690000	0.997320000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 03 Jun 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, 03 Jun 2024

[NEU] [hoch] Autodesk AutoCAD: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Autodesk AutoCAD ausnutzen, um beliebigen Programmcode auszuführen, um einen Denial-of-Service-Zustand zu erzeugen und um Dateien zu manipulieren.

- Link

—

Mon, 03 Jun 2024

[NEU] [hoch] Apache Wicket: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Mon, 03 Jun 2024

[NEU] [hoch] Apache OFBiz: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Mon, 03 Jun 2024

[UPDATE] [hoch] Ruby: Schwachstelle ermöglicht Manipulation von Dateien

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

- Link

—

Mon, 03 Jun 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um beliebigen Programmcode auszuführen Informationen offenzulegen oder einen Denial of Service zu verursachen.

- Link

—

Mon, 03 Jun 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in strongSwan ausnutzen, um beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Mon, 03 Jun 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, 03 Jun 2024

[UPDATE] [hoch] Autodesk AutoCAD: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Autodesk AutoCAD ausnutzen,

um beliebigen Programmcode auszuführen.
- Link

—

Mon, 03 Jun 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder um Sicherheitsmaßnahmen zu umgehen.
- Link

—

Mon, 03 Jun 2024

[UPDATE] [hoch] Ruby: Mehrere Schwachstellen

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

—

Mon, 03 Jun 2024

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

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

—

Mon, 03 Jun 2024

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

Ein Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren, Cross-Site Scripting (XSS)-Angriffe durchzuführen oder einen Men-in-the-Middle-Angriff auszuführen.
- Link

—

Mon, 03 Jun 2024

[UPDATE] [hoch] Google Chrome und Microsoft Edge: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen und weitere, nicht spezifizierte Auswirkungen zu verursachen.
- Link

—

Mon, 03 Jun 2024

[UPDATE] [hoch] Moodle: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Moodle ausnutzen, um beliebigen Code auszuführen, ReCAPTCHA zu umgehen, vertrauliche Informationen offenzulegen oder einen Cross-Site Scripting (XSS)-Angriff durchzuführen.

- Link

—

Mon, 03 Jun 2024

[UPDATE] [hoch] Check Point Security Gateway: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Check Point Security Gateway ausnutzen, um Informationen offenzulegen.

- Link

—

Fri, 31 May 2024

[NEU] [hoch] Harbor: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Harbor ausnutzen, um Informationen offenzulegen und um URLs zu manipulieren.

- Link

—

Fri, 31 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

—

Fri, 31 May 2024

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um einen Denial of Service Angriff durchzuführen und um Sicherheitsmechanismen zu umgehen.

- Link

—

Fri, 31 May 2024

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in git ausnutzen, um Sicherheitsvorkehrungen zu umgehen und beliebigen Code auszuführen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
6/3/2024	[RHEL 8 : binutils (Unpatched Vulnerability)]	critical
6/3/2024	[RHEL 7 : openjpeg (Unpatched Vulnerability)]	critical
6/3/2024	[RHEL 6 : pyyaml (Unpatched Vulnerability)]	critical
6/3/2024	[RHEL 4 : ipsec-tools (Unpatched Vulnerability)]	critical
6/3/2024	[RHEL 7 : ocaml (Unpatched Vulnerability)]	critical
6/3/2024	[RHEL 7 : libwebp (Unpatched Vulnerability)]	critical
6/3/2024	[RHEL 5 : firefox (Unpatched Vulnerability)]	critical
6/3/2024	[RHEL 6 : pcre (Unpatched Vulnerability)]	critical
6/3/2024	[RHEL 7 : mingw-virt-viewer (Unpatched Vulnerability)]	critical
6/3/2024	[RHEL 6 : less (Unpatched Vulnerability)]	critical
6/3/2024	[RHEL 6 : ocaml (Unpatched Vulnerability)]	critical
6/3/2024	[RHEL 6 : binutils (Unpatched Vulnerability)]	critical
6/3/2024	[RHEL 6 : firefox (Unpatched Vulnerability)]	critical
6/3/2024	[RHEL 7 : firefox (Unpatched Vulnerability)]	critical
6/3/2024	[RHEL 5 : less (Unpatched Vulnerability)]	critical
6/3/2024	[RHEL 7 : libjpeg-turbo (Unpatched Vulnerability)]	high
6/3/2024	[RHEL 7 : 389-ds-base (Unpatched Vulnerability)]	high
6/3/2024	[RHEL 5 : fontconfig (Unpatched Vulnerability)]	high
6/3/2024	[RHEL 8 : python-mako (Unpatched Vulnerability)]	high
6/3/2024	[RHEL 4 : radvd (Unpatched Vulnerability)]	high
6/3/2024	[RHEL 7 : byacc (Unpatched Vulnerability)]	high
6/3/2024	[RHEL 8 : eclipse (Unpatched Vulnerability)]	high
6/3/2024	[RHEL 6 : mingw-virt-viewer (Unpatched Vulnerability)]	high
6/3/2024	[RHEL 8 : memcached (Unpatched Vulnerability)]	high

Datum	Schwachstelle	Bewertung
6/3/2024	[RHEL 4 : binutils (Unpatched Vulnerability)]	high
6/3/2024	[RHEL 9 : mod_security (Unpatched Vulnerability)]	high
6/3/2024	[RHEL 8 : mod_security (Unpatched Vulnerability)]	high
6/3/2024	[RHEL 7 : gdk-pixbuf (Unpatched Vulnerability)]	high
6/3/2024	[Microsoft Edge (Chromium) < 125.0.2535.85 Multiple Vulnerabilities]	high
6/3/2024	[RHEL 9 : nodejs (RHSA-2024:3545)]	high
6/3/2024	[RHEL 7 : Red Hat Single Sign-On 7.6.9 security update on RHEL 7 (Low) (RHSA-2024:3566)]	high
6/3/2024	[RHEL 9 : Red Hat Single Sign-On 7.6.9 security update on RHEL 9 (Low) (RHSA-2024:3568)]	high
6/3/2024	[RHEL 8 : Red Hat Single Sign-On 7.6.9 security update on RHEL 8 (Low) (RHSA-2024:3567)]	high
6/3/2024	[RHEL 9 : nodejs:18 (RHSA-2024:3544)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Mon, 03 Jun 2024

Check Point Security Gateway Arbitrary File Read Detection Tool

This is a vulnerability detection and exploitation tool design to take in a list of targets and check for the arbitrary file read vulnerability in Check Point Security Gateways.

- Link

—

” “Mon, 03 Jun 2024

Check Point Security Gateway Arbitrary File Read

Proof of concept exploit for Check Point Security Gateways that allows an unauthenticated remote attacker to read the contents of an arbitrary file located on the affected appliance.

- Link

—

” “Mon, 03 Jun 2024

Employee And Visitor Gate Pass Logging System 1.0 SQL Injection

Employee and Visitor Gate Pass Logging System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Mon, 03 Jun 2024

FreePBX 16 Remote Code Execution

FreePBX suffers from a remote code execution vulnerability. Versions 14, 15, and 16 are all affected.

- Link

—

” “Mon, 03 Jun 2024

Sitefinity 15.0 Cross Site Scripting

Sitefinity version 15.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Mon, 03 Jun 2024

appRain CMF 4.0.5 Shell Upload

appRain CMF version 4.0.5 suffers from a remote shell upload vulnerability.

- Link

—

” “Mon, 03 Jun 2024

CMSimple 5.15 Remote Shell Upload

CMSimple version 5.15 suffers from a remote shell upload vulnerability.

- Link

—

” “Mon, 03 Jun 2024

Monstra CMS 3.0.4 Remote Code Execution

Monstra CMS version 3.0.4 suffers from a remote code execution vulnerability. Original discovery of code execution in this version is attributed to Ishaq Mohammed in December of 2017.

- Link

—

” “Mon, 03 Jun 2024

Dotclear 2.29 Remote Code Execution

Dotclear version 2.29 suffers from a remote code execution vulnerability.

- Link

—

” “Mon, 03 Jun 2024

WBCE CMS 1.6.2 Remote Code Execution

WBCE CME version 1.6.2 suffers from a remote code execution vulnerability.

- Link

—

” “Mon, 03 Jun 2024

Serendipity 2.5.0 Remote Code Execution

Serendipity version 2.5.0 suffers from a remote code execution vulnerability.

- Link

—

” “Fri, 31 May 2024

Packet Storm New Exploits For May, 2024

This archive contains all of the 68 exploits added to Packet Storm in May, 2024.

- Link

—

” “Fri, 31 May 2024

changedetection 0.45.20 Remote Code Execution

changedetection versions 0.45.20 and below suffer from a remote code execution vulnerability.

- Link

—

” “Fri, 31 May 2024

Online Payment Hub System 1.0 SQL Injection

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

- Link

—

” “Fri, 31 May 2024

BWL Advanced FAQ Manager 2.0.3 SQL Injection

BWL Advanced FAQ Manager version 2.0.3 suffers from a remote SQL injection vulnerability.

- Link

—

” “Fri, 31 May 2024

iMLog Cross Site Scripting

iMLog versions prior to 1.307 suffer from a persistent cross site scripting vulnerability.

- Link

—

” “Fri, 31 May 2024

Check Point Security Gateway Information Disclosure

Check Point Security Gateway suffers from an information disclosure vulnerability. Versions affected include R77.20 (EOL), R77.30 (EOL), R80.10 (EOL), R80.20 (EOL), R80.20.x, R80.20SP (EOL), R80.30

(EOL), R80.30SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x, and R81.20.
- Link

—

” “Thu, 30 May 2024

Aquatronica Control System 5.1.6 Password Disclosure

Aquatronica Control System version 5.1.6 has a tcp.php endpoint on the controller that is exposed to unauthenticated attackers over the network. This vulnerability allows remote attackers to send a POST request which can reveal sensitive configuration information, including plaintext passwords. This can lead to unauthorized access and control over the aquarium controller, compromising its security and potentially allowing attackers to manipulate its settings.
- Link

—

” “Thu, 30 May 2024

Progress Flowmon 12.3.5 Local sudo Privilege Escalation

This Metasploit module abuses a feature of the sudo command on Progress Flowmon. Certain binary files are allowed to automatically elevate with the sudo command. This is based off of the file name. This includes executing a PHP command with a specific file name. If the file is overwritten with PHP code it can be used to elevate privileges to root. Progress Flowmon up to at least version 12.3.5 is vulnerable.
- Link

—

” “Thu, 30 May 2024

Akaunting 3.1.8 Client-Side Template Injection

Akaunting version 3.1.8 suffers from a client-side template injection vulnerability.
- Link

—

” “Thu, 30 May 2024

Akaunting 3.1.8 Server-Side Template Injection

Akaunting version 3.1.8 suffers from a server-side template injection vulnerability.
- Link

—

” “Thu, 30 May 2024

ORing IAP-420 2.01e Cross Site Scripting / Command Injection

ORing IAP-420 version 2.01e suffers from remote command injection and persistent cross site scripting vulnerabilities.
- Link

—

” “Wed, 29 May 2024

Flowmon Unauthenticated Command Injection

This Metasploit module exploits an unauthenticated command injection vulnerability in Progress Flowmon versions before v12.03.02.

- Link

—

” “Tue, 28 May 2024

Eclipse ThreadX Buffer Overflows

Eclipse ThreadX versions prior to 6.4.0 suffers from a missing array size check causing a memory overwrite, missing parameter checks leading to integer wraparound, under allocations, heap buffer overflows, and more.

- Link

—

” “Tue, 28 May 2024

HAWKI 1.0.0-beta.1 XSS / File Overwrite / Session Fixation

HAWKI version 1.0.0-beta.1 before commit 146967f suffers from cross site scripting, arbitrary file overwrite, and session fixation vulnerabilities.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Fri, 31 May 2024

ZDI-24-562: Canon imageCLASS MF753Cdw setResource Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-561: Progress Software Telerik Reporting Register Authentication Bypass Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-560: Lexmark CX331adwe Firmware Downgrade Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-559: G DATA Total Security Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-558: G DATA Total Security Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-557: Kofax Power PDF JPF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-556: Kofax Power PDF JP2 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-555: Kofax Power PDF JP2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-554: Kofax Power PDF JP2 File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-553: Kofax Power PDF JP2 File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-552: Kofax Power PDF AcroForm Annotation Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-551: Kofax Power PDF PDF File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-550: Kofax Power PDF PDF File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-549: Kofax Power PDF TGA File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-548: Kofax Power PDF PSD File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-547: Kofax Power PDF PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-546: Kofax Power PDF PSD File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-545: (Pwn2Own) Sonos Era 100 SMB2 Message Handling Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-544: (Pwn2Own) Sonos Era 100 SMB2 Message Handling Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-543: (Pwn2Own) Sonos Era 100 SMB2 Message Handling Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-542: (Pwn2Own) Sonos Era 100 SMB2 Message Handling Integer Underflow Information Disclosure Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-541: Luxion KeyShot Viewer KSP File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-540: Luxion KeyShot BIP File Parsing Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-539: Luxion KeyShot Viewer KSP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-538: Luxion KeyShot Viewer KSP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-537: Fuji Electric Alpha5 C5V File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-536: Fuji Electric Alpha5 C5V File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-535: Fuji Electric Monitouch V-SFT V9C File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-534: Fuji Electric Monitouch V-SFT V9C File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-533: Fuji Electric Monitouch V-SFT V9C File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-532: Fuji Electric Monitouch V-SFT V10 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-531: Fuji Electric Monitouch V-SFT V9C File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-530: Fuji Electric Monitouch V-SFT V9C File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-529: (Pwn2Own) VMware Workstation UrbBuf_getDataBuf Uninitialized Variable Information Disclosure Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-528: (Pwn2Own) VMware Workstation hgfsVMCI_fileread Use of Uninitialized Variable In-

formation Disclosure Vulnerability

- Link

—

” “Fri, 31 May 2024

ZDI-24-527: (Pwn2Own) VMWare Workstation VBluetoothHCI_PacketOut Use-After-Free Privilege Escalation Vulnerability

- Link

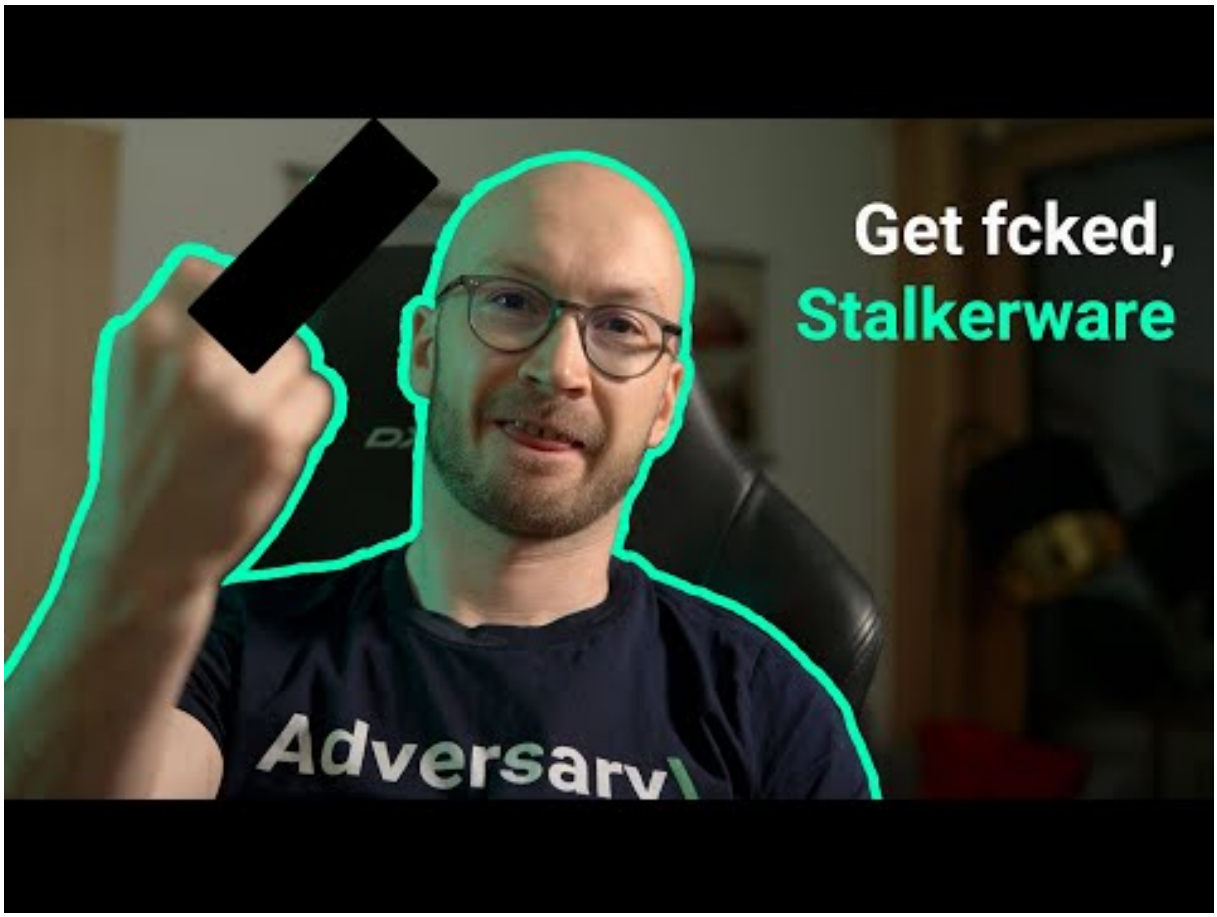
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 FCK Stalkerware.



Zum Youtube Video

6 Cyberangriffe: (Jun)

Datum	Opfer	Land	Information
2024-06-02	Institut technologique de Sonora (Itson)	[MEX]	Link

7 Ransomware-Erpressungen: (Jun)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-03	[Langescheid GbR]	arcusmedia	Link
2024-06-03	[Franja IT Integradores de Tecnología]	arcusmedia	Link
2024-06-03	[Duque Saldarriaga]	arcusmedia	Link
2024-06-03	[BHMAC]	arcusmedia	Link
2024-06-03	[Botselo]	arcusmedia	Link
2024-06-03	[Immediate Transport – UK]	arcusmedia	Link
2024-06-01	[cfymca.org]	lockbit3	Link
2024-06-03	[Northern Minerals Limited]	bianlian	Link
2024-06-03	[ISETO CORPORATION]	8base	Link
2024-06-03	[Nidec Motor Corporation]	8base	Link
2024-06-03	[Anderson Mikos Architects]	akira	Link
2024-06-03	[My City application]	handala	Link
2024-06-02	[www.eastshoresound.com]	ransomhub	Link
2024-06-02	[smithandcaugheys.co.nz]	lockbit3	Link
2024-06-01	[Frontier]	ransomhub	Link
2024-06-16	[garrettmotion.com]	dispossessor	Link
2024-06-28	[notablefrontier.com]	dispossessor	Link
2024-06-12	[energytransfer.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.