Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240205

Inhaltsverzeichnis

1 Editorial **2**

2 Security-News **3**
2.1 Heise - Security-Alert . . . 3

3 Sicherheitslücken **4**
3.1 EPSS . . . 4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit . . . 5
3.2 BSI - Warn- und Informationsdienst (WID) . . . 6
3.3 Sicherheitslücken Meldungen von Tenable . . . 10

4 Aktiv ausgenutzte Sicherheitslücken **12**
4.1 Exploits der letzten 5 Tage . . . 12
4.2 0-Days der letzten 5 Tage . . . 16

5 Die Hacks der Woche **17**
5.0.1 Microsoft kriegt IHRE EIGENE Cloud nicht sicher konfiguriert . . . 17

6 Cyberangriffe: (Feb) **18**

7 Ransomware-Erpressungen: (Feb) **18**

8 Quellen **19**
8.1 Quellenverzeichnis . . . 19

9 Impressum **20**

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

IBM Business Automation Workflow für DoS-Attacken & Co. anfällig

Mehrere Schwachstellen in IBM Business Automation Workflow gefährden Systeme.

- Link

—

IT-Sicherheitsüberwachung Juniper JSA für mehrere Attacken anfällig

Angreifer können Junipers Security-Information-and-Event-Management-System JSA ins Visier nehmen. Sicherheitspatches sind verfügbar.

- Link

—

QNAP: Neue Firmware-Versionen beheben Befehlsschmuggel-Lücke

Unter anderem konnten Angreifer aus der Ferne eigene Kommandos auf den Geräten einschleusen. Admins sollten zügig patchen.

- Link

—

Sicherheitsupdate: IBM-Sicherheitslösung QRadar SIEM unter Linux angreifbar

Mehrere Komponenten eines Add ons von IBMs Security Information and Event Management-System QRadar sind verwundbar.

- Link

—

Mastodon: Diebstahl beliebiger Identitäten im föderierten Kurznachrichtendienst

In einem knappen Sicherheitshinweis lassen die Entwickler eine Bombe platzen: Angreifer können jeden beliebigen Account übernehmen und fälschen.

- Link

—

Ivanti: Updates mit Verspätung, dafür neue Sicherheitslücke missbraucht

Ivanti hat Updates zum Schließen von Sicherheitslücken veröffentlicht, die bereits angegriffen werden. Zwei weitere Lecks sind dabei aufgetaucht.

- Link

—

Linux: Sicherheitslücke in glibc bringt Angreifern Root-Privilegien

Fast alle aktuellen Linux-Varianten sind von dem Sicherheitsleck betroffen, das Missetäter jedoch nicht aus der Ferne angreifen können. Updates stehen bereit.

- Link

—

Sicherheitsupdates: DoS- und Schadcode-Attacken auf IBM ODM möglich

Angreifer können Systeme über diverse Schwachstellen in IBM Operational Decision Manager kompromittieren.

- Link

—

Google Chrome: Update schließt vier Sicherheitslücken

Google hat mit dem wöchentlichen Chrome-Update vier Sicherheitslücken geschlossen. Sie könnten das Einschleusen von Schadcode erlauben.

- Link

—

Jetzt updaten! Exploits für kritische Jenkins-Sicherheitslücke im Umlauf

Für die in der vergangenen Woche bekanntgewordene kritische Sicherheitslücke in Jenkins ist Exploit-Code aufgetaucht. Höchste Zeit zum Aktualisieren!

- 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-2023-6553	0.909010000	0.986400000	Link
CVE-2023-5360	0.967230000	0.995900000	Link
CVE-2023-4966	0.931240000	0.988840000	Link
CVE-2023-46805	0.930450000	0.988740000	Link
CVE-2023-46747	0.970550000	0.997170000	Link
CVE-2023-46604	0.971470000	0.997610000	Link
CVE-2023-42793	0.973260000	0.998680000	Link
CVE-2023-38035	0.971870000	0.997830000	Link
CVE-2023-36845	0.967370000	0.995970000	Link
CVE-2023-35082	0.932740000	0.989070000	Link
CVE-2023-35078	0.955550000	0.992690000	Link
CVE-2023-34634	0.906880000	0.986160000	Link
CVE-2023-34362	0.952300000	0.991940000	Link
CVE-2023-33246	0.971740000	0.997730000	Link
CVE-2023-32315	0.963290000	0.994510000	Link
CVE-2023-30625	0.950540000	0.991540000	Link
CVE-2023-30013	0.925700000	0.988250000	Link
CVE-2023-29300	0.939750000	0.989880000	Link
CVE-2023-28771	0.923800000	0.987990000	Link
CVE-2023-27524	0.961820000	0.994070000	Link
CVE-2023-27372	0.970420000	0.997120000	Link
CVE-2023-27350	0.972270000	0.998090000	Link
CVE-2023-26469	0.927230000	0.988420000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-26360	0.943910000	0.990520000	Link
CVE-2023-26035	0.968710000	0.996460000	Link
CVE-2023-25717	0.956130000	0.992790000	Link
CVE-2023-25194	0.916080000	0.987070000	Link
CVE-2023-2479	0.964780000	0.994960000	Link
CVE-2023-24489	0.969290000	0.996650000	Link
CVE-2023-23752	0.963140000	0.994450000	Link
CVE-2023-23397	0.906590000	0.986140000	Link
CVE-2023-22527	0.973010000	0.998510000	Link
CVE-2023-22518	0.965250000	0.995180000	Link
CVE-2023-22515	0.956820000	0.992950000	Link
CVE-2023-21839	0.957980000	0.993170000	Link
CVE-2023-21823	0.940060000	0.989920000	Link
CVE-2023-21554	0.961220000	0.993880000	Link
CVE-2023-20887	0.961320000	0.993910000	Link
CVE-2023-20198	0.924070000	0.988040000	Link
CVE-2023-1671	0.953130000	0.992130000	Link
CVE-2023-0669	0.968210000	0.996270000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 02 Feb 2024

[NEU] [hoch] Microsoft Edge: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 02 Feb 2024

[UPDATE] [hoch] IBM QRadar SIEM User Behavior Analytics: Mehrere Schwachstellen

Ein anonymer Angreifer kann mehrere Schwachstellen in IBM QRadar SIEM User Behavior Analytics ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, einen Man-in-the-Middle-Angriff durchzuführen oder vertrauliche Informationen offenzulegen.

- Link

—

Fri, 02 Feb 2024

[UPDATE] [kritisch] D-LINK Router: Mehrere Schwachstellen ermöglichen Ausführen von beliebigem Programmcode mit Administratorrechten

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in D-LINK Router ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen.

- Link

—

Fri, 02 Feb 2024

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

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

- Link

—

Fri, 02 Feb 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

—

Fri, 02 Feb 2024

[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen

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

- Link

—

Fri, 02 Feb 2024

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

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat Satellite ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Fri, 02 Feb 2024

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

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

- Link

—

Fri, 02 Feb 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

—

Fri, 02 Feb 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

—

Fri, 02 Feb 2024

[UPDATE] [hoch] GNU libc: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in GNU libc ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Fri, 02 Feb 2024

[UPDATE] [hoch] Ivanti Connect Secure: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Ivanti Connect Secure ausnutzen, um seine Privilegien zu erhöhen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Fri, 02 Feb 2024

[UPDATE] [hoch] docker: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Docker ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder Dateien zu manipulieren.

- Link

—

Fri, 02 Feb 2024

[NEU] [hoch] D-LINK Router: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in D-LINK Router ausnutzen, um beliebigen Programmcode auszuführen oder sonstige Auswirkungen zu verursachen.
- Link

—

Thu, 01 Feb 2024

[NEU] [hoch] Rockwell Automation ControlLogix: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Rockwell Automation ControlLogix ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

Thu, 01 Feb 2024

[NEU] [hoch] Rockwell Automation FactoryTalk: Schwachstelle ermöglicht Manipulation von Dateien und Offenlegung von Informationen

Ein anonymer Angreifer kann eine Schwachstelle in Rockwell Automation FactoryTalk ausnutzen, um Dateien zu manipulieren oder vertrauliche Informationen offenzulegen.
- Link

—

Thu, 01 Feb 2024

[NEU] [hoch] D-LINK COVR-2600R & COVR-3902: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in COVR-2600R & COVR-3902 Routern ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Thu, 01 Feb 2024

[NEU] [hoch] Sparx Systems Enterprise Architect: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in Sparx Systems Enterprise Architect ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Thu, 01 Feb 2024

[NEU] [hoch] D-LINK Router: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in D-LINK Router ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Thu, 01 Feb 2024

[UPDATE] [kritisch] Apple macOS: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um den Benutzer zu täuschen, Informationen offenzulegen, Sicherheitsmechanismen zu umgehen, Rechte zu erweitern und beliebigen Code mit Kernel-Rechten auszuführen.
- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
2/4/2024	[GLSA-202402-10 : NBD Tools: Multiple Vulnerabilities]	critical
2/4/2024	[Slackware Linux 15.0 / current libxml2 Vulnerability (SSA:2024-035-01)]	critical
2/3/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : openconnect (SUSE-SU-2024:0317-1)]	critical
2/3/2024	[SUSE SLES12 Security Update : slurm_23_02 (SUSE-SU-2024:0312-1)]	critical
2/3/2024	[SUSE SLES12 Security Update : slurm_20_02 (SUSE-SU-2024:0310-1)]	critical
2/3/2024	[SUSE SLES12 Security Update : slurm (SUSE-SU-2024:0315-1)]	critical
2/3/2024	[SUSE SLES15 Security Update : slurm (SUSE-SU-2024:0314-1)]	critical
2/3/2024	[SUSE SLES12 Security Update : slurm_22_05 (SUSE-SU-2024:0311-1)]	critical
2/3/2024	[SUSE SLES12 Security Update : slurm_18_08 (SUSE-SU-2024:0313-1)]	critical
2/3/2024	[SUSE SLES12 Security Update : slurm_20_11 (SUSE-SU-2024:0309-1)]	critical
2/3/2024	[GLSA-202402-05 : Microsoft Edge: Multiple Vulnerabilities]	critical
2/3/2024	[GLSA-202402-04 : GNAT Ada Suite: Remote Code Execution]	critical

Datum	Schwachstelle	Bewertung
2/3/2024	[GLSA-202402-06 : FreeType: Multiple Vulnerabilities]	critical
2/3/2024	[Debian dsa-5614 : gir1.2-zbar-1.0 - security update]	critical
2/2/2024	[Fedora 38 : indent (2024-74667e499e)]	critical
2/2/2024	[Fedora 39 : indent (2024-bfd13103eb)]	critical
2/2/2024	[Cisco Unity Connection Arbitrary File Upload (cisco-sa-cuc-unauth-afu-FROYsCsD)]	critical
2/2/2024	[FreeBSD : chromium – multiple security fixes (72d6d757-c197-11ee-86bb-a8a1599412c6)]	critical
2/2/2024	[Ivanti Connect Secure 9.x / 22.x Authentication Bypass Vulnerability (CVE-2023-46805)]	critical
2/2/2024	[Ivanti Policy Secure 9.x / 22.x Authentication Bypass Vulnerability (CVE-2023-46805)]	critical
2/2/2024	[Ivanti Policy Secure 9.x / 22.x Command Injection Vulnerability (CVE-2024-21887)]	critical
2/2/2024	[Ivanti Connect Secure 9.x / 22.x Command Injection Vulnerability (CVE-2024-21887)]	critical
2/4/2024	[GLSA-202402-07 : Xen: Multiple Vulnerabilities]	high
2/4/2024	[GLSA-202402-08 : OpenSSL: Multiple Vulnerabilities]	high
2/4/2024	[Debian dsa-5615 : golang-github-opencontainers-runc-dev - security update]	high
2/3/2024	[SUSE SLES12 Security Update : gdb (SUSE-SU-2024:0319-1)]	high
2/3/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : xerces-c (SUSE-SU-2024:0320-1)]	high
2/3/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : java-11-openjdk (SUSE-SU-2024:0321-1)]	high
2/3/2024	[GLSA-202402-03 : QtGui: Multiple Vulnerabilities]	high
2/3/2024	[Debian dla-3732 : sudo - security update]	high
2/2/2024	[SUSE SLES15 Security Update : webkit2gtk3 (SUSE-SU-2024:0301-1)]	high

Datum	Schwachstelle	Bewertung
2/2/2024	[SUSE SLES12 Security Update : runc (SUSE-SU-2024:0294-1)]	high
2/2/2024	[SUSE SLES12 Security Update : gstreamer (SUSE-SU-2024:0307-1)]	high
2/2/2024	[SUSE SLES15 Security Update : xerces-c (SUSE-SU-2024:0300-1)]	high
2/2/2024	[SUSE SLES12 Security Update : squid (SUSE-SU-2024:0296-1)]	high
2/2/2024	[FreeBSD : electron{26,27,28} – Use after free in Web Audio (13a8c4bf-cb2b-48ec-b49c-a3875c72b3e8)]	high
2/2/2024	[FreeBSD : chromium – multiple security fixes (dc9e5237-c197-11ee-86bb-a8a1599412c6)]	high
2/2/2024	[Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2024-12110)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Fri, 02 Feb 2024

Fortra GoAnywhere MFT Unauthenticated Remote Code Execution

This Metasploit module exploits a vulnerability in Fortra GoAnywhere MFT that allows an unauthenticated attacker to create a new administrator account. This can be leveraged to upload a JSP payload and achieve RCE. GoAnywhere MFT versions 6.x from 6.0.1, and 7.x before 7.4.1 are vulnerable.

- Link

—

” “Fri, 02 Feb 2024

Juniper SRX Firewall / EX Switch Remote Code Execution

This code serves as both a vulnerability detector and a proof of concept for CVE-2023-36845. It executes the phpinfo() function on the login page of the target device, allowing to inspect the PHP configuration. This script also has the option to save the phpinfo() output to a file for further analysis.

- Link

—

” “Fri, 02 Feb 2024

PCMan FTP Server 2.0 Buffer Overflow

PCMan FTP Server version 2.0 pwn remote buffer overflow exploit.

- Link

—

” “Fri, 02 Feb 2024

Proxmox VE 7.4-1 TOTP Brute Force

Proxmox VE versions 5.4 through 7.4-1 suffer from a TOTP brute forcing vulnerability.

- Link

—

” “Fri, 02 Feb 2024

TP-LINK TL-WR740N HTML Injection

TP-LINK TL-WR740N suffers from an html injection vulnerability.

- Link

—

” “Fri, 02 Feb 2024

GoAhead Web Server 2.5 HTML Injection

GoAhead Web Server version 2.5 suffers from an html injection vulnerability.

- Link

—

” “Fri, 02 Feb 2024

ComSndFTP Server 1.3.7 Beta Denial Of Service

ComSndFTP Server version 1.3.7 Beta remote denial of service exploit.

- Link

—

” “Fri, 02 Feb 2024

Ricoh Printer Directory / File Exposure

Ricoh printers suffer from directory and file exposure vulnerabilities.

- Link

—

” “Fri, 02 Feb 2024

Typora 1.7.4 Command Injection

Typora version 1.7.4 suffers from a command injection vulnerability.

- Link

—

” “Fri, 02 Feb 2024

Bank Locker Management System SQL Injection

Bank Locker Management System suffers from a remote SQL injection vulnerability.

- Link

—

” “Fri, 02 Feb 2024

Grocy 4.0.2 Cross Site Request Forgery

Grocy versions 4.0.2 and below suffer from a cross site request forgery vulnerabilities.

- Link

—

” “Fri, 02 Feb 2024

WebCatalog 48.4 Arbitrary Protocol Execution / Code Execution

WebCatalog versions prior to 48.8 call the Electron shell.openExternal function without verifying that the URL is for an http or https resource. This vulnerability allows an attacker to potentially execute code through arbitrary protocols on the victims machine by having users sync pages with malicious URLs. The victim has to interact with the link, which can then enable an attacker to bypass security measures for malicious file delivery.

- Link

—

” “Fri, 02 Feb 2024

7 Sticky Notes 1.9 Command Injection

7 Sticky Notes version 1.9 suffers from a command injection vulnerability.

- Link

—

” “Thu, 01 Feb 2024

Packet Storm New Exploits For January, 2024

This archive contains all of the 140 exploits added to Packet Storm in January, 2024.

- Link

—

” “Thu, 01 Feb 2024

Apache Tomcat 8.5.63 / 9.0.43 HTTP Response Smuggling

Apache Tomcat suffers from a client-side de-sync vulnerability via HTTP request smuggling. Apache Tomcat versions 8.5.7 through 8.5.63 and 9.0.0-M11 through 9.0.43 are vulnerable.

- Link

—

” “Thu, 01 Feb 2024

GlobalScape Secure FTP Server 3.0 Denial Of Service

GlobalScape Secure FTP Server version 3.0 remote denial of service exploit.

- Link

—

” “Wed, 31 Jan 2024

XenForo 2.2.13 ArchiveImport.php Zip Slip

XenForo versions 2.2.13 and below suffer from a zip slip filename traversal vulnerability in ArchiveImport.php.

- Link

—

” “Wed, 31 Jan 2024

TELSAT marKoni FM Transmitter 1.9.5 Insecure Access Control

TELSAT marKoni FM Transmitter version 1.9.5 allows an unauthorized user to change passwords.

- Link

—

” “Wed, 31 Jan 2024

TELSAT marKoni FM Transmitter 1.9.5 Client-Side Access Control Bypass

TELSAT marKoni FM Transmitter version 1.9.5 implements client-side restrictions that can be bypassed by editing the HTML source page that enable administrative operations.

- Link

—

” “Wed, 31 Jan 2024

TELSAT marKoni FM Transmitter 1.9.5 Backdoor Account

TELSAT marKoni FM Transmitter version 1.9.5 has a hidden super administrative account factory that has the hardcoded password inokram25 that allows full access to the web management interface configuration.

- Link

—

” “Wed, 31 Jan 2024

TELSAT marKoni FM Transmitter 1.9.5 Root Command Injection

TELSAT marKoni FM Transmitter version 1.9.5 is susceptible to unauthenticated remote code execution with root privileges. An attacker can exploit a command injection vulnerability by manipulating the Email settings’ WAN IP info service, which utilizes the wget module. This allows the attacker to gain unauthorized access to the system with administrative privileges by exploiting the url parameter in the HTTP GET request to ekafcgi.fcgi.

- Link

—

” “Wed, 31 Jan 2024

glibc syslog() Heap-Based Buffer Overflow

Qualys discovered a heap-based buffer overflow in the GNU C Library’s __vsyslog_internal() function, which is called by both syslog() and vsyslog(). This vulnerability was introduced in glibc 2.37 (in August 2022).

- Link

—

” “Wed, 31 Jan 2024

glibc qsort() Out-Of-Bounds Read / Write

Qualys discovered a memory corruption in the glibc’s qsort() function, due to a missing bounds check. To be vulnerable, a program must call qsort() with a nontransitive comparison function (a function cmp(int a, int b) that returns (a - b), for example) and with a large number of attacker-controlled elements (to cause a malloc() failure inside qsort()). They have not tried to find such a vulnerable program in the real world. All glibc versions from at least September 1992 (glibc 1.04) to the current release (glibc 2.38) are affected, but the glibc’s developers have independently discovered and patched this memory corruption in the master branch (commit b9390ba, ”stdlib: Fix array bounds protection in insertion sort phase of qsort”) during a recent refactoring of qsort().

- Link

—

” “Wed, 31 Jan 2024

Trojan.Win32 BankShot MVID-2024-0669 Buffer Overflow

Trojan.Win32 BankShot malware suffers from a buffer overflow vulnerability.

- Link

—

” “Wed, 31 Jan 2024

War-FTPD 1.65 Denial Of Service

War-FTPD version 1.65 remote denial of service exploit.

- Link

—

”

4.2 0-Days der letzten 5 Tage

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Microsoft kriegt IHRE EIGENE Cloud nicht sicher konfiguriert

Zum Youtube Video

6 Cyberangriffe: (Feb)

Datum	Opfer	Land	Information
2024-02-02	Germantown	[USA]	Link
2024-02-02	Université de Reykjavík	[ISL]	Link
2024-02-01	Landkreis Kelheim	[DEU]	Link
2024-02-01	Groton Public Schools	[USA]	Link
2024-02-01	Diagnostic Medical Systems Group (DMS Group)	[FRA]	Link

7 Ransomware-Erpressungen: (Feb)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-04	[DOD contractors you are welcome in our chat.]	donutleaks	Link
2024-02-04	[cxm.com]	lockbit3	Link
2024-02-04	[Cole, Cole, Easley & Sciba]	bianlian	Link
2024-02-04	[Commonwealth Sign]	qilin	Link
2024-02-04	[FEPCO Zona Franca SAS]	knight	Link
2024-02-03	[pbwtulsa.com]	lockbit3	Link
2024-02-02	[Digitel Venezuela]	medusa	Link
2024-02-02	[Chaney, Couch, Callaway, Carter & Associates Family Dentistry.]	bianlian	Link
2024-02-02	[manitou-group.com]	lockbit3	Link
2024-02-02	[AbelSantosyAsociados]	knight	Link
2024-02-02	[lexcaribbean.com]	lockbit3	Link
2024-02-02	[Law Office of Michael H Joseph]	bianlian	Link
2024-02-02	[Tandem]	bianlian	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-02	[Innovex Downhole Solutions]	play	Link
2024-02-01	[CityDfDefiance(Disclosure of all)]	knight	Link
2024-02-01	[DIROX LTDA (Vietnã)]	knight	Link
2024-02-01	[etsolutions.com.mx]	threeam	Link
2024-02-01	[gatesshields.com]	lockbit3	Link
2024-02-01	[manchesterfertility.com]	lockbit3	Link
2024-02-01	[stemcor.com]	lockbit3	Link
2024-02-01	[Borah Goldstein Altschuler Nahins & Goidel]	akira	Link
2024-02-01	[dms-imaging]	cuba	Link
2024-02-01	[bandcllp.com]	lockbit3	Link
2024-02-01	[taloninternational.com]	lockbit3	Link
2024-02-01	[Southwark Council]	meow	Link
2024-02-01	[Robert D. Clements Jr Law Group, LLLP]	bianlian	Link
2024-02-01	[CNPC Peru S.A.]	rhysida	Link
2024-02-01	[Primeimaging database for sale]	everest	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.