Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241008

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

Sicherheitsupdates: Cisco patcht Lücken in Produkten quer durch die Bank

Neben einem kritischen Fehler kümmert sich der Netzwerkausrüster auch um einige Lücken mit mittlerem und hohem Risikograd. Patches stehen bereit.

- Link

—

Zimbra: Codeschmuggel-Lücke wird angegriffen

In der Kollaborationssoftware Zimbra klafft eine Sicherheitslücke, die Angreifer bereits aktiv missbrauchen. Admins sollten zügig updaten.

- Link

—

Web-Config von Seiko-Epson-Geräten ermöglicht Angreifern Übernahme

Das Web-Interface von Geräten wie Druckern von Seiko-Epson ermöglicht Angreifern in vielen Fällen, diese als Administrator zu übernehmen.

- Link

—

CERT-Bund warnt: Mehr als 15.000 Exchange-Server mit Sicherheitslücken

In Deutschland stehen noch immer mehr als 15.000 Exchange-Server mit mindestens einer Codeschmuggel-Lücke offen im Netz, warnt das CERT-Bund.

- Link

—

Monitoring-Software Whatsup Gold: Hersteller rät zum schleunigen Update

Progress warnt, dass teils kritische Sicherheitslücken in Whatsup Gold lauern. Admins sollen so schnell wie möglich aktualisieren.

- Link

—

Kritische Sicherheitslücken: PHP 8.3.12, 8.2.24 und 8.1.30 dichten Lecks ab

Die PHP-Entwickler haben PHP 8.3.12, 8.2.24 und 8.1.30 veröffentlicht. Darin schließen sie mehrere, teils kritische Sicherheitslücken.

- Link

—

Foxit PDF: Manipulierte PDFs können Schadcode durchschleusen

Es sind gegen verschiedene Attacken gerüstete Versionen von Foxit PDF Editor und PDF Reader für macOS und Windows erschienen.

- Link

—

Teils kritische Lücken in Unix-Drucksystem CUPS ermöglichen Codeschmuggel

Im Linux-Drucksystem CUPS wurden teils kritische Sicherheitslücken entdeckt. Angreifer können dadurch etwa Code einschmuggeln.

- Link

—

Schadcode-Schlupfloch in Nvidia Container Toolkit geschlossen

Angreifer können an Sicherheitslücken in Nvidia Container Toolkit und GPU Operator ansetzen, um Systeme zu kompromittieren.

- Link

—

Sicherheitsupdates: DoS-Angriffe auf Cisco-Netzwerkhardware möglich

Aufgrund von mehreren Sicherheitslücken in Ciscos Netzwerkbetriebssystem IOS XE sind verschiedene Geräte verwundbar. Patches stehen zum Download.

- 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	0.957580000	0.994840000	Link
CVE-2023-6895	0.927330000	0.990830000	Link
CVE-2023-6553	0.947820000	0.993210000	Link
CVE-2023-6019	0.933510000	0.991430000	Link
CVE-2023-52251	0.949200000	0.993410000	Link
CVE-2023-4966	0.970840000	0.998180000	Link
CVE-2023-49103	0.949680000	0.993510000	Link
CVE-2023-48795	0.964670000	0.996230000	Link
CVE-2023-47246	0.960360000	0.995280000	Link
CVE-2023-46805	0.960890000	0.995410000	Link
CVE-2023-46747	0.971910000	0.998530000	Link
CVE-2023-46604	0.970850000	0.998180000	Link
CVE-2023-4542	0.944110000	0.992660000	Link
CVE-2023-43208	0.974200000	0.999500000	Link
CVE-2023-43177	0.954700000	0.994380000	Link
CVE-2023-42793	0.970970000	0.998240000	Link
CVE-2023-41892	0.904950000	0.989080000	Link
CVE-2023-41265	0.907590000	0.989260000	Link
CVE-2023-39143	0.940700000	0.992260000	Link
CVE-2023-38205	0.951890000	0.993880000	Link
CVE-2023-38203	0.964750000	0.996280000	Link
CVE-2023-38146	0.919150000	0.990050000	Link
CVE-2023-38035	0.974600000	0.999680000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.967920000	0.997200000	Link
CVE-2023-3519	0.965910000	0.996610000	Link
CVE-2023-35082	0.967900000	0.997190000	Link
CVE-2023-35078	0.969440000	0.997620000	Link
CVE-2023-34993	0.973450000	0.999160000	Link
CVE-2023-34960	0.900520000	0.988820000	Link
CVE-2023-34634	0.923140000	0.990430000	Link
CVE-2023-34362	0.970450000	0.998040000	Link
CVE-2023-34105	0.927500000	0.990860000	Link
CVE-2023-34039	0.943770000	0.992610000	Link
CVE-2023-3368	0.934610000	0.991560000	Link
CVE-2023-33246	0.970550000	0.998070000	Link
CVE-2023-32315	0.971490000	0.998400000	Link
CVE-2023-30625	0.953820000	0.994240000	Link
CVE-2023-30013	0.965950000	0.996620000	Link
CVE-2023-29300	0.967820000	0.997150000	Link
CVE-2023-29298	0.969430000	0.997610000	Link
CVE-2023-28432	0.921930000	0.990320000	Link
CVE-2023-28343	0.957650000	0.994850000	Link
CVE-2023-28121	0.922260000	0.990350000	Link
CVE-2023-27524	0.969670000	0.997700000	Link
CVE-2023-27372	0.973980000	0.999410000	Link
CVE-2023-27350	0.968980000	0.997480000	Link
CVE-2023-26469	0.953540000	0.994180000	Link
CVE-2023-26360	0.964630000	0.996220000	Link
CVE-2023-26035	0.967750000	0.997120000	Link
CVE-2023-25717	0.950620000	0.993640000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-25194	0.964550000	0.996190000	Link
CVE-2023-2479	0.963230000	0.995870000	Link
CVE-2023-24489	0.972860000	0.998920000	Link
CVE-2023-23752	0.949000000	0.993380000	Link
CVE-2023-23333	0.960430000	0.995290000	Link
CVE-2023-22527	0.970410000	0.998020000	Link
CVE-2023-22518	0.959950000	0.995230000	Link
CVE-2023-22515	0.973910000	0.999370000	Link
CVE-2023-21839	0.941470000	0.992350000	Link
CVE-2023-21554	0.952650000	0.994040000	Link
CVE-2023-20887	0.970950000	0.998230000	Link
CVE-2023-1698	0.917150000	0.989880000	Link
CVE-2023-1671	0.962220000	0.995650000	Link
CVE-2023-0669	0.971830000	0.998500000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 07 Oct 2024

[UPDATE] [hoch] CUPS: Mehrere Schwachstellen ermöglichen Ausführung von beliebigem Programmcode

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in CUPS ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen und um Informationen offenzulegen.

- Link

—

Mon, 07 Oct 2024

[NEU] [hoch] HP Computer: Schwachstelle ermöglicht Privilegieneskalation

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

- Link

—

Mon, 07 Oct 2024

[NEU] [UNGEPATCHT] [hoch] Samsung Exynos: Schwachstelle ermöglicht Privilegieneskalation

Ein Angreifer kann eine Schwachstelle in Samsung Exynos ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Mon, 07 Oct 2024

[NEU] [hoch] MediaWiki: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in MediaWiki ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Cross-Site-Scripting-Angriff durchzuführen oder Dateien zu manipulieren.

- Link

—

Mon, 07 Oct 2024

[NEU] [hoch] DrayTek Vigor Router: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in DrayTek Vigor Routern ausnutzen, um beliebigen Code auszuführen, Cross-Site-Scripting-Angriffe durchzuführen, vertrauliche Informationen preiszugeben und einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Mon, 07 Oct 2024

[UPDATE] [hoch] Red Hat Enterprise Linux (python-setuptools): Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 07 Oct 2024

[UPDATE] [hoch] Eclipse Jetty: Mehrere Schwachstellen ermöglichen Denial of Service

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Eclipse Jetty ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Mon, 07 Oct 2024

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer oder ein lokaler authentifizierter Angreiferkann mehrere Schwachstellen in git ausnutzen, um beliebigen Programmcode auszuführen und und die Sicher-

heitsmaßnahmen zu umgehen.

- Link

—

Mon, 07 Oct 2024

[UPDATE] [hoch] Mozilla Firefox, Firefox ESR und Thunderbird: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um einen Spoofing-Angriff durchzuführen, beliebigen Code auszuführen, Dateien zu manipulieren, vertrauliche Informationen offenzulegen oder Cross-Site-Scripting-Angriffe durchzuführen.

- Link

—

Mon, 07 Oct 2024

[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

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

- Link

—

Mon, 07 Oct 2024

[UPDATE] [hoch] Mozilla Firefox, Firefox ESR und Thunderbird: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Thunderbird ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmaßnahmen zu umgehen, Daten zu manipulieren, einen Denial-of-Service-Zustand zu erzeugen und vertrauliche Informationen preiszugeben.

- Link

—

Mon, 07 Oct 2024

[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

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

- Link

—

Fri, 04 Oct 2024

[NEU] [hoch] Xerox FreeFlow Core: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Xerox FreeFlow Core ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 04 Oct 2024

[NEU] [UNGEPATCHT] [hoch] Cisco Small Business: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Cisco Small Business ausnutzen, um seine Privilegien zu erhöhen, beliebige Befehle auszuführen und einen Denial of Service-Zustand zu verursachen.

- Link

—

Fri, 04 Oct 2024

[NEU] [hoch] Cisco Nexus Dashboard und Nexus Dashboard Fabric Controller: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Cisco Nexus Dashboard ausnutzen, um Informationen offenzulegen Sicherheitsmaßnahmen zu umgehen und beliebigen Code, im schlimmsten Fall mit Administratorrechten, zur Ausführung zu bringen.

- Link

—

Fri, 04 Oct 2024

[NEU] [hoch] Jenkins: Mehrere Schwachstellen

Ein entfernter, authentisierter oder anonymer Angreifer kann mehrere Schwachstellen in Jenkins und verschiedenen Jenkins Plugins ausnutzen, um Informationen offenzulegen Sicherheitsvorkehrungen zu umgehen oder seine Rechte zu erweitern.

- Link

—

Fri, 04 Oct 2024

[NEU] [hoch] CUPS: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in CUPS cups-browsed ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Fri, 04 Oct 2024

[UPDATE] [hoch] ImageMagick: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in ImageMagick ausnutzen, um einen Denial of Service Angriff durchzuführen, vertrauliche Daten einzusehen oder weitere Angriffe mit nicht beschriebenen Auswirkungen durchzuführen.

- Link

—

Fri, 04 Oct 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht nicht spezifizierten Angriff
Ein Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.
- Link
—
Fri, 04 Oct 2024
[UPDATE] [hoch] UnZip: Mehrere Schwachstellen ermöglichen Codeausführung
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in UnZip ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.
- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
10/7/2024	[Fedora 39 : firefox (2024-86edbf4d85)]	critical
10/7/2024	[Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-7056-1)]	critical
10/7/2024	[RHEL 8 : thunderbird (RHSA-2024:7699)]	critical
10/7/2024	[Oracle Linux 8 : thunderbird (ELSA-2024-7699)]	critical
10/4/2024	[AlmaLinux 9 : firefox (ALSA-2024:7505)]	critical
10/4/2024	[Debian dsa-5783 : firefox-esr - security update]	critical
10/4/2024	[Amazon Linux AMI : amazon-ssm-agent (ALAS-2024-1948)]	critical
10/7/2024	[Ubuntu 16.04 LTS : CUPS vulnerability (USN-7041-3)]	high
10/7/2024	[Nutanix AOS : Multiple Vulnerabilities (NXSA-AOS-6.10)]	high
10/7/2024	[Ubuntu 24.04 LTS : WEBrick vulnerability (USN-7057-1)]	high
10/7/2024	[Oracle Linux 7 : python3-setuptools (ELSA-2024-6661)]	high
10/7/2024	[RHEL 8 : firefox (RHSA-2024:7703)]	high
10/7/2024	[RHEL 7 / 8 / 9 : Red Hat JBoss Enterprise Application Platform 7.4 Security update (Important) (RHSA-2024:7736)]	high

Datum	Schwachstelle	Bewertung
10/7/2024	[RHEL 8 : git (RHSA-2024:7701)]	high
10/7/2024	[RHEL 7 : systemd (RHSA-2024:7705)]	high
10/7/2024	[RHEL 8 : firefox (RHSA-2024:7700)]	high
10/7/2024	[RHEL 8 : firefox (RHSA-2024:7704)]	high
10/7/2024	[RHEL 7 : firefox (RHSA-2024:7702)]	high
10/7/2024	[Debian dla-3912 : ata-modules-5.10.0-29-armmp-di - security update]	high
10/7/2024	[Oracle Linux 8 : firefox (ELSA-2024-7700)]	high
10/6/2024	[Fedora 40 : p7zip (2024-5c99e1d579)]	high
10/6/2024	[Fedora 39 : chromium (2024-7aba3c1531)]	high
10/6/2024	[Fedora 39 : aws (2024-d940f25a53)]	high
10/6/2024	[Fedora 40 : aws (2024-63f98f8c60)]	high
10/6/2024	[CBL Mariner 2.0 Security Update: heimdal (CVE-2022-3116)]	high
10/6/2024	[CBL Mariner 2.0 Security Update: python3 (CVE-2024-4032)]	high
10/6/2024	[CBL Mariner 2.0 Security Update: hyperv-daemons (CVE-2024-27397)]	high
10/6/2024	[Debian dla-3911 : gir1.2-gsf-1 - security update]	high
10/5/2024	[Fedora 40 : chromium (2024-452b60addf)]	high
10/5/2024	[SUSE SLES15 Security Update : openssl-3 (SUSE-SU-2024:3525-1)]	high
10/5/2024	[SUSE SLES15 Security Update : frr (SUSE-SU-2024:3524-1)]	high
10/5/2024	[FreeBSD : zeek – potential DoS vulnerability (fe7031d3-3000-4b43-9fa6-52c2b624b8f9)]	high
10/5/2024	[Debian dsa-5786 : gir1.2-gsf-1 - security update]	high
10/4/2024	[Debian dla-3910 : comerr-dev - security update]	high
10/4/2024	[Debian dsa-5784 : liboath-dev - security update]	high
10/4/2024	[Amazon Linux AMI : kernel (ALAS-2024-1947)]	high
10/4/2024	[Oracle Linux 7 : e2fsprogs (ELSA-2024-12704)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Mon, 07 Oct 2024

Grav CMS 1.7.44 Server-Side Template Injection

GenGravSSTIExploit is a proof of concept Python script that exploits an authenticated server-side template injection (SSTI) vulnerability in Grav CMS versions 1.7.44 and below. This vulnerability allows a user with editor permissions to execute OS commands on a remote server.

- Link

—

” “Mon, 07 Oct 2024

Ruby-SAML / GitLab Authentication Bypass

This script exploits the issue noted in CVE-2024-45409 that allows an unauthenticated attacker with access to any signed SAML document issued by the IDP to forge a SAML Response/Assertion and gain access as any user on GitLab. Ruby-SAML versions below or equal to 12.2 and versions 1.13.0 through 1.16.0 do not properly verify the signature of the SAML Response.

- Link

—

” “Mon, 07 Oct 2024

iTunes For Windows 12.13.2.3 Local Privilege Escalation

This is a thorough write up of how to exploit a local privilege escalation vulnerability in iTunes for Windows version 12.13.2.3. Apple fixed this in version 12.13.3.

- Link

—

” “Mon, 07 Oct 2024

ABB Cylon Aspect 3.08.00 syslogSwitch.php Remote Code Execution

ABB Cylon Aspect versions 3.08.00 and below suffer from an authenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the SYSLOG HTTP POST parameter called by the syslogSwitch.php script.

- Link

—

” “Mon, 07 Oct 2024

ABB Cylon Aspect 3.08.01 caldavUtil.php Remote Code Execution

ABB Cylon Aspect versions 3.08.01 and below suffer from an unauthenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the Footer HTTP POST parameter called by the caldavUtil.php script.

- Link

—

” “Mon, 07 Oct 2024

ABB Cylon Aspect 3.08.00 setTimeServer.php Remote Code Execution

ABB Cylon Aspect versions 3.08.00 and below suffer from an authenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the timeserver HTTP POST parameter called by the setTimeServer.php script.

- Link

—

” “Mon, 07 Oct 2024

ABB Cylon Aspect 3.08.01 logYumLookup.php Unauthenticated File Disclosure

ABB Cylon Aspect versions 3.08.01 and below suffer from an unauthenticated arbitrary file disclosure vulnerability. Input passed through the logFile GET parameter via the logYumLookup.php script is not properly verified before being used to download log files. This can be exploited to disclose the contents of arbitrary and sensitive files via directory traversal attacks.

- Link

—

” “Mon, 07 Oct 2024

Book Recording App 2024-09-24 Cross Site Scripting

Book Recording App, as submitted on 2024-09-24, suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Mon, 07 Oct 2024

OpenMediaVault 7.4.2-2 Code Injection

OpenMediaVault version 7.4.2-2 suffers from a PHP code injection vulnerability.

- Link

—

” “Mon, 07 Oct 2024

Netis MW5360 Code Injection

Netis MW5360 suffers from a PHP code injection vulnerability.

- Link

—

” “Mon, 07 Oct 2024

Hikvision IP Camera Cross Site Request Forgery

Hikvision IP Cameras suffer from a cross site request forgery vulnerability.

- Link

—

” “Mon, 07 Oct 2024

GeoServer 2.25.1 Code Injection

GeoServer version 2.25.1 suffers from a PHP code injection vulnerability.

- Link

—

” “Mon, 07 Oct 2024

Gambio Online Webshop 4.9.2.0 Code Injection

Gambio Online Webshop version 4.9.2.0 suffers from a PHP code injection vulnerability.

- Link

—

” “Fri, 04 Oct 2024

ABB Cylon Aspect 3.07.02 Authenticated File Disclosure

ABB Cylon Aspect version 3.07.02 suffers from an authenticated arbitrary file disclosure vulnerability. Input passed through the file GET parameter through the downloadDb.php script is not properly verified before being used to download database files. This can be exploited to disclose the contents of arbitrary and sensitive files via directory traversal attacks.

- Link

—

” “Fri, 04 Oct 2024

TeamViewer Privilege Escalation

Proof of concept code for a flaw in TeamViewer that enables an unprivileged user to load an arbitrary kernel driver into the system.

- Link

—

” “Fri, 04 Oct 2024

MD-Pro 1.0.76 Shell Upload / SQL Injection

MD-Pro version 1.0.76 suffers from remote SQL injection and shell upload vulnerabilities.

- Link

—

” “Fri, 04 Oct 2024

Computer Laboratory Management System 2024 1.0 Cross Site Scripting

Computer Laboratory Management System 2024 version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Fri, 04 Oct 2024

Acronis Cyber Infrastructure 5.0.1-61 Cross Site Request Forgery

Acronis Cyber Infrastructure version 5.0.1-61 suffers from a cross site request forgery vulnerability.

- Link

—

” “Fri, 04 Oct 2024

Vehicle Service Management System 1.0 WYSIWYG Code Injection

Vehicle Service Management System version 1.0 suffers from a WYSIWYG code injection vulnerability.

- Link

—

” “Fri, 04 Oct 2024

Vehicle Service Management System 1.0 Code Injection

Vehicle Service Management System version 1.0 suffers from a PHP code injection vulnerability.

- Link

—

” “Fri, 04 Oct 2024

Transport Management System 1.0 Arbitrary File Upload

Transport Management System version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Fri, 04 Oct 2024

Transport Management System 1.0 Code Injection

Transport Management System version 1.0 suffers from a PHP code injection vulnerability.

- Link

—

” “Fri, 04 Oct 2024

ManageEngine ADManager 7183 Password Hash Disclosure

ManageEngine ADManager version 7183 suffers from a password hash disclosure vulnerability.

- Link

—

” “Fri, 04 Oct 2024

fastrpc_mmap_create Use-After-Free

A condition exists when fastrpc_mmap_create creates a new globally visible mapping that can lead to a use-after-free.

- Link

—

” “Thu, 03 Oct 2024

Acronis Cyber Infrastructure Default Password Remote Code Execution

Acronis Cyber Infrastructure (ACI) is an IT infrastructure solution that provides storage, compute, and network resources. Businesses and Service Providers are using it for data storage, backup storage, creating and managing virtual machines and software-defined networks, running cloud-native applications in production environments. This Metasploit module exploits a default password vulnerability

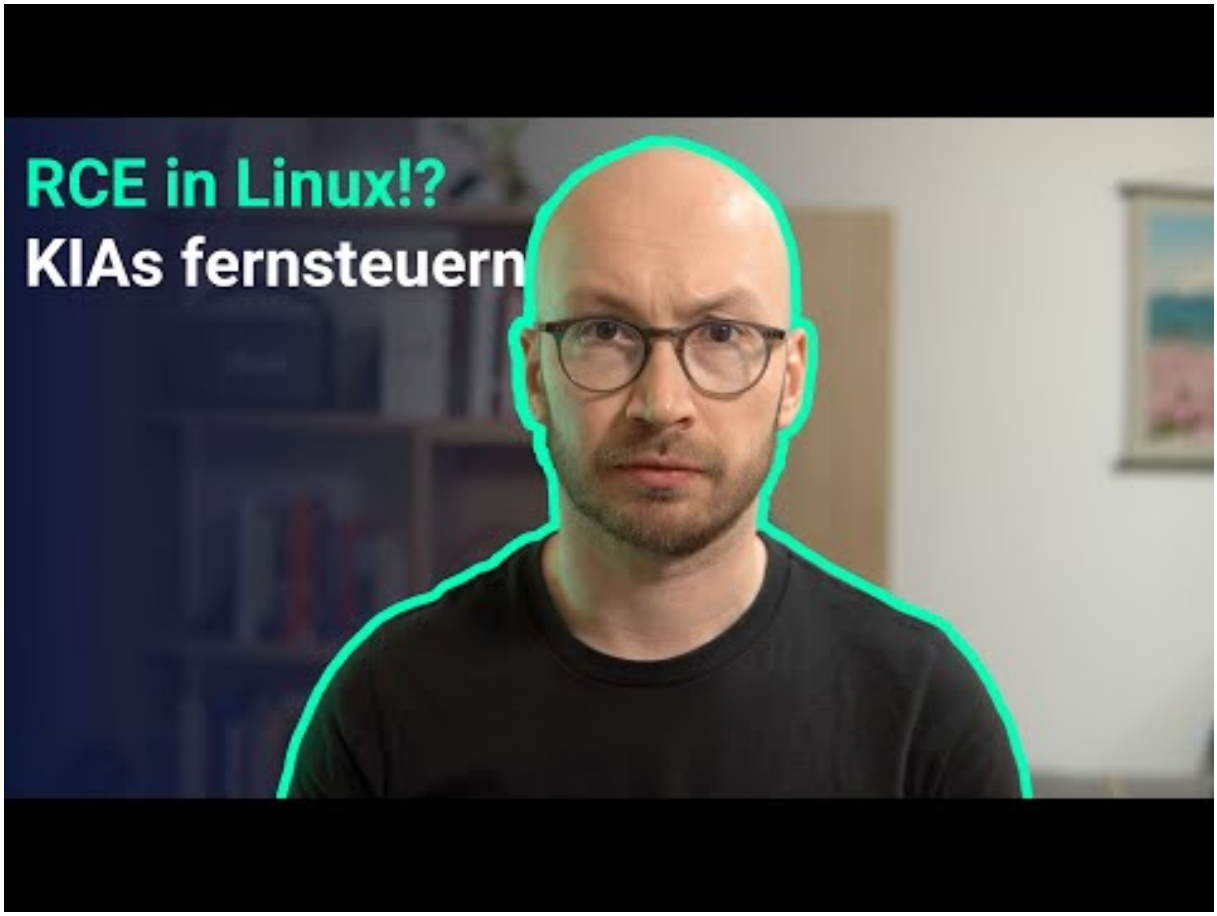
in ACI which allow an attacker to access the ACI PostgreSQL database and gain administrative access to the ACI Web Portal. This opens the door for the attacker to upload SSH keys that enables root access to the appliance/server. This attack can be remotely executed over the WAN as long as the PostgreSQL and SSH services are exposed to the outside world. ACI versions 5.0 before build 5.0.1-61, 5.1 before build 5.1.1-71, 5.2 before build 5.2.1-69, 5.3 before build 5.3.1-53, and 5.4 before build 5.4.4-132 are vulnerable.
- Link
—
”

4.2 0-Days der letzten 5 Tage

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Ein Grund mehr, Drucker zu hassen. Und Autos.



Zum Youtube Video

6 Cyberangriffe: (Okt)

Datum	Opfer	Land	Information
2024-10-04	Groupe Hospi Grand Ouest	[FRA]	Link
2024-10-03	Uttarakhand	[IND]	Link
2024-10-03	American Water Works	[USA]	Link
2024-10-02	Thoraxzentrum Bezirk Unterfranken	[DEU]	Link
2024-10-02	Wayne County	[USA]	Link
2024-10-02	Traffics GmbH	[DEU]	Link
2024-10-01	Oyonnax	[FRA]	Link

7 Ransomware-Erpressungen: (Okt)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-07	[Istrail]	medusa	Link
2024-10-07	[Albany College of Pharmacy]	medusa	Link
2024-10-07	[Arelance Group]	medusa	Link
2024-10-08	[Pearl Cohen]	bianlian	Link
2024-10-07	[Broward Realty Corp]	everest	Link
2024-10-07	[yassir.com]	killsec	Link
2024-10-03	[tpgagedcare.com.au]	lockbit3	Link
2024-10-06	[IIB (Israeli Industrial Batteries) Leaked]	handala	Link
2024-10-03	[lyra.officegroup.it]	stormous	Link
2024-10-05	[AOSense/NASA]	stormous	Link
2024-10-05	[NASA/AOSense]	stormous	Link
2024-10-05	[Creative Consumer Concepts]	play	Link
2024-10-05	[Power Torque Services]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-05	[seoulpi.io]	killsec	Link
2024-10-05	[canstarrestorations.com]	ransomhub	Link
2024-10-05	[www.ravencm.com]	ransomhub	Link
2024-10-05	[Ibermutuamur]	hunters	Link
2024-10-05	[betterhalf.ai]	killsec	Link
2024-10-05	[HARTSON-KENNEDY.COM]	clop	Link
2024-10-04	[omniboxx.nl]	ransomhub	Link
2024-10-05	[BNBuilders]	hunters	Link
2024-10-04	[winwinza.com]	ransomhub	Link
2024-10-04	[Storck-Baugesellschaft mbH]	incransom	Link
2024-10-04	[C&L Ward]	play	Link
2024-10-04	[Wilmington Convention Center]	play	Link
2024-10-04	[Guerriere & Halnon]	play	Link
2024-10-04	[Markdom Plastic Products]	play	Link
2024-10-04	[Pete’s Road Service]	play	Link
2024-10-04	[releese.io]	ransomhub	Link
2024-10-04	[kleberandassociates.com]	ransomhub	Link
2024-10-04	[City Of Forest Park - Full Leak]	monti	Link
2024-10-04	[Riley Gear Corporation]	akira	Link
2024-10-04	[TANYA Creations]	akira	Link
2024-10-04	[mullenwylie.com]	ElDorado	Link
2024-10-04	[GenPro Inc.]	blacksuit	Link
2024-10-04	[CopySmart LLC]	ciphbit	Link
2024-10-04	[North American Breaker]	akira	Link
2024-10-04	[Amplitude Laser]	hunters	Link
2024-10-04	[GW Mechanical]	hunters	Link
2024-10-04	[Dreyfuss + Blackford Architecture]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-04	[Transtec SAS]	orca	Link
2024-10-02	[enterpriseoutsourcing.com]	ransomhub	Link
2024-10-04	[DPC DATA]	qilin	Link
2024-10-03	[Lyomark Pharma]	dragonforce	Link
2024-10-03	[Conductive Containers, Inc]	cicada3301	Link
2024-10-04	[bbgc.gov.bd]	killsec	Link
2024-10-03	[CobelPlast]	hunters	Link
2024-10-03	[Shin Bet]	handala	Link
2024-10-03	[Barnes & Cohen]	trinity	Link
2024-10-03	[TRC Worldwide Engineering (Trcww)]	akira	Link
2024-10-03	[Rob Levine & Associates (roblevine.com)]	akira	Link
2024-10-03	[Red Barrels]	nitrogen	Link
2024-10-03	[CaleyWray]	hunters	Link
2024-10-03	[LIFTING.COM]	clop	Link
2024-10-01	[Emerson]	medusa	Link
2024-10-03	[Golden Age Nursing Home]	rhysida	Link
2024-10-02	[mccartycompany.com]	ransomhub	Link
2024-10-02	[bypeterandpauls.com]	ransomhub	Link
2024-10-02	[domainindustries.com]	ransomhub	Link
2024-10-02	[ironmetals.com]	ransomhub	Link
2024-10-02	[rollxvans.com]	ransomhub	Link
2024-10-02	[ETC Companies]	akira	Link
2024-10-02	[Branhaven Chrysler Dodge Jeep Ram]	blacksuit	Link
2024-10-02	[Holmes & Brakel]	akira	Link
2024-10-02	[Forshey Prostok LLP]	qilin	Link
2024-10-02	[Israel Prime Minister Emails]	handala	Link
2024-10-02	[FoccoERP]	trinity	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-01	[Quantum Healthcare]	incransom	Link
2024-10-01	[Acuity Advisor]	stormous	Link
2024-10-01	[United Animal Health]	qilin	Link
2024-10-01	[Akromold]	nitrogen	Link
2024-10-01	[Labib Funk Associates]	nitrogen	Link
2024-10-01	[Research Electronics International]	nitrogen	Link
2024-10-01	[Cascade Columbia Distribution]	akira	Link
2024-10-01	[ShoreMaster]	akira	Link
2024-10-01	[marthamedeiros.com.br]	madliberator	Link
2024-10-01	[CSG Consultants]	akira	Link
2024-10-01	[aberdeenwa.gov]	ElDorado	Link
2024-10-01	[Corantioquia]	meow	Link
2024-10-01	[performance-therapies]	qilin	Link
2024-10-01	[www.galab.com]	cactus	Link
2024-10-01	[telehealthcenter.in]	killsec	Link
2024-10-01	[howardcpas.com]	ElDorado	Link
2024-10-01	[bshsoft.com]	ElDorado	Link
2024-10-01	[credihealth.com]	killsec	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.