Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240125

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

Codeschmuggel-Lücke in HPE Oneview

Mehrere Sicherheitslücken in der IT-Infrastrukturverwaltung HPE Oneview ermöglichen Angreifern, etwa Schadcode einzuschleusen. Updates stehen bereit.

- Link

—

Firefox: Passkey-Unterstützung und Sicherheitsfixes

Die Version 122 von Firefox kann mit Passkeys umgehen. Außerdem schließen die Entwickler darin wie in Firefox ESR und Thunderbird 115.7 Sicherheitslecks.

- Link

—

Fortra GoAnywhere MFT: Kritische Lücke macht Angreifer zu Admins

Jetzt patchen! Es ist Exploitcode für die Dateiübertragungslösung Fortra GoAnywhere MFT in Umlauf.

- Link

—

Chrome-Update dichtet 17 Sicherheitslecks ab

Googles Entwickler aktualisieren den Chrome-Webbrowser und schließen 17 Sicherheitslücken darin. Einige ermöglichen wohl Codeschmuggel.

- Link

—

Barracuda WAF: Kritische Sicherheitslücken ermöglichen Umgehung des Schutzes

Barracuda hat einen Sicherheitshinweis bezüglich der Web Application Firewall veröffentlicht. Sicherheitslücken ermöglichen das Umgehen des Schutzes.

- Link

—

Monitoringsoftware Splunk: Teils kritische Sicherheitslücken

Splunk hat für die gleichnamige Monitoringsoftware Updates veröffentlicht. Sie dichten Sicherheitslücken darin ab.

- Link

—

Sicherheitsfixes: Apple aktualisiert ältere Systeme – und räumt Zero Days ein

Apple hat neben macOS 14.3 und iOS 17.3 auch neue Versionen von iOS 15, 16, macOS 12 und 13 sowie Safari veröffentlicht. Es gab einen erneuten Zero-Day-Exploit.

- Link

—

Confluence: Kritische Sicherheitslücke in veralteten Versionen wird ausgenutzt
Cybergangster durchforsten das Netz, auf der Suche nach angreifbaren Confluence-Installationen. Wer jetzt nicht handelt, riskiert Datenverluste.
- Link

—

Sicherheitsupdates: Schlupflöcher für Schadcode in Lexmark-Druckern geschlossen
Angreifer können an vielen Druckermodellen von Lexmark ansetzen, um Geräte zu kompromittieren. Derzeit soll es noch keine Attacken geben.
- Link

—

Kritische VMware-Sicherheitslücke wird angegriffen
Ende Oktober hat VMware ein Update gegen eine kritische Sicherheitslücke herausgegeben. Inzwischen wird das Leck angegriffen.
- 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	0.986260000	Link
CVE-2023-5360	0.967230000	0.995870000	Link
CVE-2023-4966	0.925220000	0.988000000	Link
CVE-2023-46805	0.930450000	0.988650000	Link
CVE-2023-46747	0.965530000	0.995280000	Link
CVE-2023-46604	0.971470000	0.997630000	Link
CVE-2023-42793	0.973260000	0.998690000	Link
CVE-2023-38035	0.971870000	0.997810000	Link
CVE-2023-35082	0.924480000	0.987910000	Link
CVE-2023-35078	0.953380000	0.992110000	Link
CVE-2023-34634	0.906880000	0.986020000	Link
CVE-2023-34362	0.954180000	0.992300000	Link
CVE-2023-33246	0.971270000	0.997540000	Link
CVE-2023-32315	0.963290000	0.994470000	Link
CVE-2023-30625	0.937630000	0.989530000	Link
CVE-2023-30013	0.925700000	0.988080000	Link
CVE-2023-29300	0.936380000	0.989350000	Link
CVE-2023-28771	0.923800000	0.987830000	Link
CVE-2023-27524	0.962690000	0.994240000	Link
CVE-2023-27372	0.969410000	0.996710000	Link
CVE-2023-27350	0.972430000	0.998160000	Link
CVE-2023-26469	0.931020000	0.988720000	Link
CVE-2023-26360	0.940990000	0.989950000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-26035	0.968020000	0.996210000	Link
CVE-2023-25717	0.956130000	0.992740000	Link
CVE-2023-25194	0.916080000	0.986910000	Link
CVE-2023-2479	0.958820000	0.993320000	Link
CVE-2023-24489	0.968380000	0.996310000	Link
CVE-2023-23752	0.963140000	0.994420000	Link
CVE-2023-22518	0.965250000	0.995140000	Link
CVE-2023-22515	0.956820000	0.992890000	Link
CVE-2023-21839	0.957980000	0.993140000	Link
CVE-2023-21823	0.940060000	0.989830000	Link
CVE-2023-21554	0.961220000	0.993850000	Link
CVE-2023-20887	0.962660000	0.994240000	Link
CVE-2023-1671	0.953130000	0.992050000	Link
CVE-2023-0669	0.968210000	0.996260000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 24 Jan 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 24 Jan 2024

[NEU] [hoch] Fortra GoAnywhere MFT: Schwachstelle ermöglicht das erlangen von Administratorrechten

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Fortra GoAnywhere MFT ausnutzen, um Administratorrechte zu erlangen

- Link

—

Wed, 24 Jan 2024

[NEU] [hoch] HPE OneView: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in HPE OneView ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, um seine Privilegien zu erweitern oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Wed, 24 Jan 2024

[UPDATE] [hoch] Ruby: Mehrere Schwachstellen

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

- Link

—

Wed, 24 Jan 2024

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

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

- Link

—

Wed, 24 Jan 2024

[UPDATE] [hoch] Apple iOS und Apple iPadOS: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS ausnutzen, um beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.

- Link

—

Wed, 24 Jan 2024

[NEU] [hoch] Mozilla Firefox: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, seine Rechte zu erweitern oder einen Phishing-Angriff durchzuführen.

- Link

—

Wed, 24 Jan 2024

[UPDATE] [hoch] python-cryptography: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

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

- Link

—

Wed, 24 Jan 2024

[UPDATE] [hoch] OpenSSL: Mehrere Schwachstellen ermöglichen Denial of Service

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in OpenSSL ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.

- Link

—

Wed, 24 Jan 2024

[UPDATE] [kritisch] Grafana: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

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

- Link

—

Wed, 24 Jan 2024

[UPDATE] [hoch] Grafana: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Grafana ausnutzen, um Informationen offenzulegen.

- Link

—

Wed, 24 Jan 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um einen Denial of Service Angriff durchzuführen oder Code zur Ausführung zu bringen.

- Link

—

Wed, 24 Jan 2024

[UPDATE] [hoch] Grafana: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Grafana ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen, um Administratorrechte zu erlangen und um Informationen offenzulegen.

- Link

—

Wed, 24 Jan 2024

[UPDATE] [hoch] Python: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Python ausnutzen, um beliebigen

Programmcode auszuführen.
- Link

—

Wed, 24 Jan 2024

[UPDATE] [hoch] Grafana: Mehrere Schwachstellen

Ein entfernter, authentisierter oder anonymer Angreifer kann mehrere Schwachstellen in Grafana ausnutzen, um Benutzerrechte zu erlangen, seine Privilegien zu erweitern und um Informationen offenzulegen.
- Link

—

Wed, 24 Jan 2024

[UPDATE] [hoch] Grafana: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Grafana ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen, Informationen falsch darzustellen und seine Privilegien zu erweitern.
- Link

—

Wed, 24 Jan 2024

[UPDATE] [hoch] Grafana: Schwachstelle ermöglicht Übernahme von Benutzerkonto

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Grafana ausnutzen, um ein Benutzerkonto zu übernehmen.
- Link

—

Wed, 24 Jan 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.
- Link

—

Wed, 24 Jan 2024

[UPDATE] [hoch] Splunk Splunk Enterprise: Mehrere Schwachstellen

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in Splunk Splunk Enterprise ausnutzen, um beliebigen Code auszuführen, einen ‘Denial of Service’-Zustand zu verursachen, seine Privilegien zu erweitern und weitere, nicht spezifizierte Auswirkungen zu verursachen.
- Link

—

Wed, 24 Jan 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
1/24/2024	[RHCOS 4 : OpenShift Container Platform 4.9.56 (RHSA-2023:0777)]	critical
1/24/2024	[RHCOS 4 : OpenShift Container Platform 4.13.3 (RHSA-2023:3536)]	critical
1/24/2024	[RHCOS 4 : Red Hat OpenShift Enterprise (RHSA-2023:3910)]	critical
1/24/2024	[RHCOS 4 : OpenShift Container Platform 4.12.20 (RHSA-2023:3409)]	critical
1/24/2024	[RHCOS 4 : OpenShift Container Platform 4.13.4 (RHSA-2023:3612)]	critical
1/24/2024	[Google Chrome < 121.0.6167.85 Multiple Vulnerabilities]	critical
1/24/2024	[Google Chrome < 121.0.6167.85 Multiple Vulnerabilities]	critical
1/24/2024	[Jenkins LTS < 2.426.3 / Jenkins weekly < 2.442 Multiple Vulnerabilities]	critical
1/24/2024	[Debian dsa-5606 : firefox-esr - security update]	critical
1/24/2024	[Debian dsa-5605 : thunderbird - security update]	critical
1/24/2024	[Debian dla-3717 : zabbix-agent - security update]	critical
1/24/2024	[Fedora 39 : firefox (2024-14dea9640b)]	critical
1/24/2024	[RHEL 9 : php:8.1 (RHSA-2024:0387)]	critical
1/24/2024	[RHEL 9 : kpatch-patch (RHSA-2024:0340)]	critical
1/24/2024	[RHCOS 4 : OpenShift Container Platform 4.11.46 (RHSA-2023:4312)]	high

Datum	Schwachstelle	Bewertung
1/24/2024	[RHCOS 4 : OpenShift Container Platform 4.11.34 (RHSA-2023:1503)]	high
1/24/2024	[RHCOS 4 : OpenShift Container Platform 4.11.52 (RHSA-2023:5717)]	high
1/24/2024	[RHCOS 4 : OpenShift Container Platform 4.10.61 (RHSA-2023:3362)]	high
1/24/2024	[RHCOS 4 : OpenShift Container Platform 4.12.0 (RHSA-2022:7398)]	high
1/24/2024	[RHCOS 4 : OpenShift Container Platform 4.13.1 (RHSA-2023:3303)]	high
1/24/2024	[RHCOS 4 : OpenShift Container Platform 4.12.3 (RHSA-2023:0727)]	high
1/24/2024	[RHCOS 4 : OpenShift Container Platform 4.12.30 (RHSA-2023:4674)]	high
1/24/2024	[RHCOS 4 : OpenShift Container Platform 4.12.45 (RHSA-2023:7610)]	high
1/24/2024	[RHCOS 4 : OpenShift Container Platform 4.13.23 (RHSA-2023:7325)]	high
1/24/2024	[RHCOS 4 : OpenShift Container Platform 4.10.67 (RHSA-2023:4898)]	high
1/24/2024	[RHCOS 4 : OpenShift Container Platform 4.12.6 (RHSA-2023:1033)]	high
1/24/2024	[RHCOS 4 : OpenShift Container Platform 4.14.4 (RHSA-2023:7473)]	high
1/24/2024	[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS : Apache::Session::LDAP vulnerability (USN-6596-1)]	high
1/24/2024	[Amazon Linux 2 : java-1.8.0-amazon-corretto (ALASCORRETTO8-2024-010)]	high
1/24/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.15-2024-035)]	high
1/24/2024	[Amazon Linux 2 : postgresql (ALASPOSTGRESQL13-2024-005)]	high

Datum	Schwachstelle	Bewertung
1/24/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.4-2024-058)]	high
1/24/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.10-2024-047)]	high
1/24/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.15-2024-034)]	high
1/24/2024	[Amazon Linux 2 : containerd (ALASDOCKER-2024-035)]	high
1/24/2024	[Amazon Linux 2 : postgresql (ALASPOSTGRESQL14-2024-004)]	high
1/24/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.10-2024-046)]	high
1/24/2024	[Amazon Linux 2 : firefox (ALASFIREFOX-2024-020)]	high
1/24/2024	[Amazon Linux 2 : containerd (ALASNITRO-ENCLAVES-2024-035)]	high
1/24/2024	[Amazon Linux 2 : postgresql (ALASPOSTGRESQL12-2024-007)]	high
1/24/2024	[Amazon Linux 2 : libpq (ALASPOSTGRESQL14-2024-005)]	high
1/24/2024	[Oracle Linux 8 : java-1.8.0-openjdk (ELSA-2024-0265)]	high
1/24/2024	[Fedora 38 : dotnet7.0 (2024-248d2135eb)]	high
1/24/2024	[Fedora 39 : dotnet7.0 (2024-b09647af24)]	high
1/24/2024	[Fedora 39 : fonttools (2024-6d1d9f70d2)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Wed, 24 Jan 2024

GL.iNet Unauthenticated Remote Command Execution

A command injection vulnerability exists in multiple GL.iNet network products, allowing an attacker to inject and execute arbitrary shell commands via JSON parameters at the gl_system_log and gl_crash_log interface in the logread module. This Metasploit exploit requires post-authentication using the Admin-Token cookie/sessionID (SID), typically stolen by the attacker. However, by chaining this exploit with vulnerability CVE-2023-50919, one can bypass the Nginx authentication through a Lua string pattern matching and SQL injection vulnerability. The Admin-Token cookie/SID can be

retrieved without knowing a valid username and password. Many products are vulnerable.
- Link

—

” “Wed, 24 Jan 2024

Saltstack Minion Payload Deployer

This Metasploit exploit module uses saltstack salt to deploy a payload and run it on all targets which have been selected (default all). Currently only works against nix targets.
- Link

—

” “Wed, 24 Jan 2024

Employee Management System 1.0 SQL Injection

Employee Management System version 1.0 suffers from a remote SQL injection vulnerability.
- Link

—

” “Wed, 24 Jan 2024

MiniWeb HTTP Server 0.8.19 Denial Of Service

MiniWeb HTTP Server version 0.8.19 remote denial of service exploit.
- Link

—

” “Wed, 24 Jan 2024

GoAnywhere MFT Authentication Bypass

GoAnywhere MFT authentication bypass proof of concept exploit.
- Link

—

” “Tue, 23 Jan 2024

PRTG Authenticated Remote Code Execution

This Metasploit module exploits an authenticated remote code execution vulnerability in PRTG.
- Link

—

” “Tue, 23 Jan 2024

Solar FTP Server 2.1.2 Denial Of Service

Solar FTP Server version 2.1.2 remote denial of service exploit.
- Link

—

” “Mon, 22 Jan 2024

MajorDoMo Command Injection

This Metasploit module exploits a command injection vulnerability in MajorDoMo versions before 0662e5e.

- Link

—

” “Mon, 22 Jan 2024

Ivanti Connect Secure Unauthenticated Remote Code Execution

This Metasploit module chains an authentication bypass vulnerability and a command injection vulnerability to exploit vulnerable instances of either Ivanti Connect Secure or Ivanti Policy Secure, to achieve unauthenticated remote code execution. All currently supported versions 9.x and 22.x prior to the vendor mitigation are vulnerable. It is unknown if unsupported versions 8.x and below are also vulnerable.

- Link

—

” “Mon, 22 Jan 2024

EzServer 6.4.017 Denial Of Service

EzServer version 6.4.017 remote denial of service exploit.

- Link

—

” “Mon, 22 Jan 2024

xbtitFM 4.1.18 SQL Injection / Shell Upload / Traversal

xbtitFM versions 4.1.18 and below suffer from remote shell upload, remote SQL injection, and path traversal vulnerabilities.

- Link

—

” “Mon, 22 Jan 2024

Golden FTP Server 2.02b Denial Of Service

Golden FTP Server version 2.02b remote denial of service exploit.

- Link

—

” “Mon, 22 Jan 2024

Traceroute 2.1.2 Privilege Escalation

In Traceroute versions 2.0.12 through to 2.1.2, the wrapper scripts mishandle shell metacharacters, which can lead to privilege escalation if the wrapper scripts are executed via sudo. The affected wrapper scripts include tcptraceroute, tracepath, traceproto, and traceroute-nanog. Version 2.1.3 addresses this issue.

- Link

—

” “Mon, 22 Jan 2024

TrojanSpy Win32 Nivdort MVID-2024-0668 Insecure Permissions

TrojanSpy Win32 Nivdort malware suffers from an insecure permissions vulnerability.

- Link

—

” “Mon, 22 Jan 2024

ProSysInfo TFTP Server TFTPDWIN 0.4.2 Denial Of Service

ProSysInfo TFTP Server TFTPDWIN version 0.4.2 remote denial of service exploit.

- Link

—

” “Fri, 19 Jan 2024

Apache Commons Text 1.9 Remote Code Execution

This Metasploit module exploit takes advantage of the StringSubstitutor interpolator class, which is included in the Commons Text library. A default interpolator allows for string lookups that can lead to remote code execution. This is due to a logic flaw that makes the script, dns and url lookup keys interpolated by default, as opposed to what it should be, according to the documentation of the StringLookupFactory class. Those keys allow an attacker to execute arbitrary code via lookups primarily using the script key. In order to exploit the vulnerabilities, the following requirements must be met: Run a version of Apache Commons Text from version 1.5 to 1.9, use the StringSubstitutor interpolator, and the target should run JDK versions prior to 15.

- Link

—

” “Fri, 19 Jan 2024

Linux 5.6 io_uring Cred Refcount Overflow

Linux versions 5.6 and above appear to suffer from a cred refcount overflow when handling approximately 39 gigabytes of memory usage via io_uring.

- Link

—

” “Fri, 19 Jan 2024

Lepton CMS 7.0.0 Remote Code Execution

Lepton CMS version 7.0.0 suffers from a remote code execution vulnerability.

- Link

—

” “Fri, 19 Jan 2024

Firefox 121 / Chrome 120 Denial Of Service

Firefox version 121 and Chrome version 120 may both suffer from a minor denial of service issue with file downloads.

- Link

—

” “Fri, 19 Jan 2024

MiniWeb HTTP Server 0.8.1 Denial Of Service

MiniWeb HTTP Server version 0.8.1 remote denial of service exploit.

- Link

—

” “Thu, 18 Jan 2024

WordPress Backup Migration 1.3.7 Remote Command Execution

This Metasploit module exploits an unauthenticated remote command execution vulnerability in WordPress Backup Migration plugin versions 1.3.7 and below. The vulnerability is exploitable through the Content-Dir header which is sent to the /wp-content/plugins/backup-backup/includes/backup-heart.php endpoint. The exploit makes use of a neat technique called PHP Filter Chaining which allows an attacker to prepend bytes to a string by continuously chaining character encoding conversions. This allows an attacker to prepend a PHP payload to a string which gets evaluated by a require statement, which results in command execution.

- Link

—

” “Thu, 18 Jan 2024

Ansible Agent Payload Deployer

This exploit module creates an ansible module for deployment to nodes in the network. It creates a new yaml playbook which copies our payload, chmods it, then runs it on all targets which have been selected (default all).

- Link

—

” “Thu, 18 Jan 2024

SpyCamLizard 1.230 Denial Of Service

SpyCamLizard version 1.230 remote denial of service exploit.

- Link

—

” “Thu, 18 Jan 2024

Legends Of IdleOn Random Number Generation Manipulation

Legends of IdleOn suffers from use of an insecure random number generator that can be replaced by a malicious user.

- Link

—

” “Wed, 17 Jan 2024

Easy File Sharing FTP 3.6 Denial Of Service

Easy File Sharing FTP version 3.6 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 “Wir sind SeCurItY HeRsTelLeR”... jaja, geh wieder schlafen

Zum Youtube Video

6 Cyberangriffe: (Jan)

Datum	Opfer	Land	Information
2024-01-24	Comté de Washington, Pennsylvanie	[USA]	Link
2024-01-23	Département de la Sarthe	[FRA]	Link
2024-01-23	Kansas City Area Transportation Authority (KCATA)	[USA]	Link
2024-01-22	EquiLend	[USA]	Link
2024-01-22	Volkshochschule (VHS) Minden-Bad Oeynhausen	[DEU]	Link
2024-01-21	Bucks County	[USA]	Link
2024-01-20	Caravan and Motorhome Club (CAMC)	[GBR]	Link
2024-01-19	Town of Greater Napanee	[CAN]	Link
2024-01-19	Tietoevry	[SWE]	Link
2024-01-19	Clackamas Community College	[USA]	Link
2024-01-19	Japan Food Holdings	[SGP]	Link
2024-01-17	Donau 3 FM	[DEU]	Link
2024-01-17	Service de secours de Jämtland	[SWE]	Link
2024-01-17	V.I. Lottery (Loterie des Îles Vierges)	[VIR]	Link
2024-01-17	Veolia North America	[USA]	Link
2024-01-16	Université d'État du Kansas (K-State)	[USA]	Link
2024-01-15	Foxsemicon Integrated Technology Inc (□□□□)	[TWN]	Link
2024-01-15	Canterbury City Council, Thanet District Council, Dover District Council.	[GBR]	Link
2024-01-14	Douglas County Libraries	[USA]	Link
2024-01-13	Calvia	[ESP]	Link
2024-01-13	Sambr'Habitat	[BEL]	Link
2024-01-10	RE&S Holdings	[JPN]	Link
2024-01-10	Lush	[GBR]	Link

Datum	Opfer	Land	Information
2024-01-06	loanDepot	[USA]	Link
2024-01-06	Banque nationale d'Angola	[AGO]	Link
2024-01-05	Toronto Zoo	[CAN]	Link
2024-01-05	ODAV AG	[DEU]	Link
2024-01-04	City of Beckley	[USA]	Link
2024-01-04	Tigo Business	[PRY]	Link
2024-01-01	Commune de Saint-Philippe	[FRA]	Link

7 Ransomware-Erpressungen: (Jan)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-24	[Brightstar Care]	alphv	Link
2024-01-24	[Hawbaker Engineering]	ransomhouse	Link
2024-01-24	[Charles Trent]	hunters	Link
2024-01-24	[Innovative Automation]	hunters	Link
2024-01-24	[Tamdown]	hunters	Link
2024-01-24	[Thorite Group]	hunters	Link
2024-01-23	[US government (private data)]	snatch	Link
2024-01-24	[icn-artem.com]	lockbit3	Link
2024-01-24	[SANDALAWOFFICES.COM]	clop	Link
2024-01-24	[IntegrityInc.org Integrity Inc]	mydata	Link
2024-01-24	[https://www.carri.com]	mydata	Link
2024-01-24	[https://www.gadotbio.com/ Gadot Biochemical Industries Ltd]	mydata	Link
2024-01-24	[accolade-group.com + levelwear.com +Taiwan microelectronics(CRM).]	mydata	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-24	[a24group.com ambition24hours.co.za]	mydata	Link
2024-01-24	[https://www.mikeferry.com]	mydata	Link
2024-01-24	[Dirig Sheet Metal]	akira	Link
2024-01-24	[Winona Pattern & Mold]	meow	Link
2024-01-24	[Signature Performance Insurance]	medusa	Link
2024-01-24	[MBC Law Professional Corporation]	alphv	Link
2024-01-24	[Groupe Sweetco]	8base	Link
2024-01-24	[Bikesportz Imports]	8base	Link
2024-01-24	[La Ligue]	8base	Link
2024-01-24	[Midwest Service Center]	8base	Link
2024-01-24	[Sunfab Hydraulics AB]	8base	Link
2024-01-24	[Glimstedt]	8base	Link
2024-01-19	[FULL LEAK! Busse & Busee, PC Attorneys at Law]	alphv	Link
2024-01-23	[synergyfinancialgrp.com]	abyss	Link
2024-01-23	[micrometals.com]	abyss	Link
2024-01-23	[lyonshipyard.com]	lockbit3	Link
2024-01-23	[sierrafrontgroup.com]	lockbit3	Link
2024-01-23	[Cryopak]	akira	Link
2024-01-23	[fairmontfcu.com]	blackbasta	Link
2024-01-23	[ktbslaw.com]	blackbasta	Link
2024-01-23	[dupont-restauration.fr]	blackbasta	Link
2024-01-23	[kivibros.com]	blackbasta	Link
2024-01-23	[haes.ca]	blackbasta	Link
2024-01-23	[cinfab.com]	blackbasta	Link
2024-01-23	[prudentpublishing.com]	blackbasta	Link
2024-01-23	[unitedindustries.co.nz]	blackbasta	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-23	[stemcor.com]	blackbasta	Link
2024-01-23	[Wilhoit Properties]	akira	Link
2024-01-23	[Milestone Environmental Contracting]	akira	Link
2024-01-23	[Total Air Solutions]	alphv	Link
2024-01-22	[Double Eagle Energy Holdings IV]	hunters	Link
2024-01-23	[R.C. Moore Trucking]	hunters	Link
2024-01-23	[envea.global]	blackbasta	Link
2024-01-23	[Herrs (You have 72 hours)]	alphv	Link
2024-01-21	[Smith Capital - Press Release]	monti	Link
2024-01-16	[ARPEGE]	8base	Link
2024-01-09	[C and F Packing Company Inc.]	8base	Link
2024-01-22	[HOE Pharmaceuticals Sdn Bhd]	ransomhouse	Link
2024-01-22	[davidsbridal.com]	lockbit3	Link
2024-01-22	[agc.com]	blackbasta	Link
2024-01-22	[Double Eagle Development]	hunters	Link
2024-01-22	[southernwater.co.uk]	blackbasta	Link
2024-01-22	[Waldner’s]	medusa	Link
2024-01-22	[Pozzi Italy]	medusa	Link
2024-01-22	[The Gainsborough Bath]	medusa	Link
2024-01-22	[Richmond Fellowship Scotland]	medusa	Link
2024-01-22	[ANS COMPUTER [72hrs]]	alphv	Link
2024-01-18	[deknudtframes.be]	cuba	Link
2024-01-21	[synnex-grp.com]	lockbit3	Link
2024-01-21	[gattoplaters.com]	lockbit3	Link
2024-01-21	[duconind.com]	lockbit3	Link
2024-01-21	[wittmann.at]	lockbit3	Link
2024-01-21	[qtc-energy.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-21	[hughessupplyco.com]	lockbit3	Link
2024-01-21	[umi-tiles.com]	lockbit3	Link
2024-01-21	[cct.or.th]	lockbit3	Link
2024-01-22	[cmmt.com.tw]	lockbit3	Link
2024-01-21	[shenandoahtx.us]	lockbit3	Link
2024-01-21	[stjohnrochester.org]	lockbit3	Link
2024-01-21	[bmc-cpa.com]	lockbit3	Link
2024-01-21	[jasman.com.mx]	lockbit3	Link
2024-01-21	[North Star Tax And Accounting]	bianlian	Link
2024-01-21	[KC Pharmaceuticals]	bianlian	Link
2024-01-21	[Martinaire Aviation]	bianlian	Link
2024-01-21	[subway.com]	lockbit3	Link
2024-01-21	[tvjahnrheine.de]	lockbit3	Link
2024-01-21	[marxan.es]	lockbit3	Link
2024-01-21	[home-waremmien.be]	lockbit3	Link
2024-01-20	[wendy.mx]	lockbit3	Link
2024-01-20	[swiftair.com]	lockbit3	Link
2024-01-20	[Worthen Industries [You have three days]]	alphv	Link
2024-01-19	[Anna Jaques Hospital]	moneymessage	Link
2024-01-19	[pratt.edu]	lockbit3	Link
2024-01-19	[seiu1000.org]	lockbit3	Link
2024-01-19	[Sykes Consulting, Inc.]	incransom	Link
2024-01-19	[dywidag.com]	lockbit3	Link
2024-01-19	[TPG Architecture]	play	Link
2024-01-12	[jdbchina.com]	lockbit3	Link
2024-01-19	[Hamilton-Madison House]	akira	Link
2024-01-19	[Hydratek]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-19	[Busse & Busee, PC Attorneys at Law]	alphv	Link
2024-01-19	[evit.edu]	lockbit3	Link
2024-01-19	[Alupar Investimento SA]	hunters	Link
2024-01-19	[PROJECTSW]	qilin	Link
2024-01-19	[foxsemicon.com]	lockbit3	Link
2024-01-09	[Malongo France]	8base	Link
2024-01-18	[Samuel Sekuritas Indonesia & Samuel Aset Manajemen]	trigona	Link
2024-01-18	[Premier Facility Management]	trigona	Link
2024-01-18	[Fertility North]	trigona	Link
2024-01-18	[Vision Plast]	trigona	Link
2024-01-18	[uffs.edu.br]	stormous	Link
2024-01-18	[Groveport Madison Schools]	blacksuit	Link
2024-01-18	[GROWTH by NCRC]	bianlian	Link
2024-01-18	[LT Business Dynamics]	bianlian	Link
2024-01-18	[digipwr.com]	lockbit3	Link
2024-01-18	[jaffeandasher.com]	lockbit3	Link
2024-01-18	[Gallup McKinley County Schools]	hunters	Link
2024-01-15	[aercap.com]	slug	Link
2024-01-17	[DENHAM the Jeanmaker]	akira	Link
2024-01-17	[Stone, Avant & Daniels]	medusa	Link
2024-01-17	[JspPharma]	insane	Link
2024-01-16	[Axfast AB]	8base	Link
2024-01-16	[Syndicat Général des Vignerons de la Champagne]	8base	Link
2024-01-16	[Washtech]	8base	Link
2024-01-16	[SIVAM Coatings S.p.A.]	8base	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-16	[Nexus Telecom Switzerland AG]	8base	Link
2024-01-16	[millgate.co.uk]	lockbit3	Link
2024-01-16	[Becker Logistics]	akira	Link
2024-01-16	[Bestway Sales]	akira	Link
2024-01-16	[TGS Transportation]	akira	Link
2024-01-16	[Premium Guard]	akira	Link
2024-01-16	[F J O'Hara & Sons]	qilin	Link
2024-01-16	[Donear Industries]	bianlian	Link
2024-01-15	[Beit Handesai]	malekteam	Link
2024-01-15	[shinwajpn.co.jp]	lockbit3	Link
2024-01-15	[maisonsdelavenir.com]	lockbit3	Link
2024-01-15	[vasudhapharma.com]	lockbit3	Link
2024-01-15	[hosted-it.co.uk]	lockbit3	Link
2024-01-15	[Ausa]	hunters	Link
2024-01-15	[Republic Shipping Consolidators, Inc]	bianlian	Link
2024-01-15	[Northeast Spine and Sports Medicine's]	bianlian	Link
2024-01-14	[SPARTAN Light Metal Products]	unsafe	Link
2024-01-14	[Hartl European Transport Company]	unsafe	Link
2024-01-14	[American International College]	unsafe	Link
2024-01-14	[www.kai.id "FF"]	stormous	Link
2024-01-14	[amenitek.com]	lockbit3	Link
2024-01-08	[turascandinavia.com]	lockbit3	Link
2024-01-13	[Lee Spring]	rhysida	Link
2024-01-11	[Charm Sciences]	snatch	Link
2024-01-11	[Malabar Gold & Diamonds]	snatch	Link
2024-01-11	[Banco Promerica]	snatch	Link
2024-01-12	[arrowinternational.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-12	[thecsi.com]	threeam	Link
2024-01-12	[pharrusa.com]	threeam	Link
2024-01-12	[Builcore]	alphv	Link
2024-01-12	[hotelcontinental.no]	qilin	Link
2024-01-12	[olea.com]	lockbit3	Link
2024-01-12	[asburyauto.com]	cactus	Link
2024-01-12	[Washington School For The Deaf]	incransom	Link
2024-01-12	[Former S.p.A.]	8base	Link
2024-01-12	[International Trade Brokers and Forwarders]	8base	Link
2024-01-12	[BALLAY MENUISERIES]	8base	Link
2024-01-12	[Anderson King Energy Consultants, LLC]	8base	Link
2024-01-12	[Sems and Specials Incorporated]	8base	Link
2024-01-12	[acutis.com]	cactus	Link
2024-01-12	[dtsolutions.net]	cactus	Link
2024-01-12	[intercityinvestments.com]	cactus	Link
2024-01-12	[hi-cone.com]	cactus	Link
2024-01-12	[Alliedwoundcare]	everest	Link
2024-01-12	[Primeimaging]	everest	Link
2024-01-11	[Blackburn College]	akira	Link
2024-01-11	[Vincentz Network]	akira	Link
2024-01-11	[Limburg]	medusa	Link
2024-01-11	[Water For People]	medusa	Link
2024-01-11	[pactchangeslives.com]	lockbit3	Link
2024-01-11	[Triella]	alphv	Link
2024-01-11	[Ursel Phillips Fellows Hopkinson]	alphv	Link
2024-01-11	[SHIBLEY RIGHTON]	alphv	Link
2024-01-11	[automotionshade.com]	alphv	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-11	[R Robertson Insurance Brokers]	alphv	Link
2024-01-10	[molnar&partner]	qilin	Link
2024-01-10	[hartalega.com.my]	lockbit3	Link
2024-01-10	[agnesb.eu]	lockbit3	Link
2024-01-10	[twt.co.za]	lockbit3	Link
2024-01-10	[tiautoinvestments.co.za]	lockbit3	Link
2024-01-10	[Group Bogart]	alphv	Link
2024-01-09	[Delco Automation]	blacksuit	Link
2024-01-09	[Viridi]	akira	Link
2024-01-09	[Ito Pallpack Gruppen]	akira	Link
2024-01-09	[Corinth Coca-Cola Bottling Works]	qilin	Link
2024-01-09	[Precision Tune Auto Care]	8base	Link
2024-01-08	[Erbilbil Bilgisayar]	alphv	Link
2024-01-08	[HALLEONARD]	qilin	Link
2024-01-08	[Van Buren Public Schools]	akira	Link
2024-01-08	[Heller Industries]	akira	Link
2024-01-08	[CellNetix Pathology & Laboratories, LLC]	incransom	Link
2024-01-08	[mciwv.com]	lockbit3	Link
2024-01-08	[morganpilate.com]	lockbit3	Link
2024-01-07	[capitalhealth.org]	lockbit3	Link
2024-01-07	[Flash-Motors Last Warning]	raznatovic	Link
2024-01-07	[Agro Baggio LTDA]	knight	Link
2024-01-06	[Maas911.com]	cloak	Link
2024-01-06	[GRUPO SCA]	knight	Link
2024-01-06	[Televerde]	play	Link
2024-01-06	[The Lutheran World Federation]	rhysida	Link
2024-01-05	[Proax Technologies LTD]	bianlian	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-05	[Somerset Logistics]	bianlian	Link
2024-01-05	[ips-securex.com]	lockbit3	Link
2024-01-04	[Project M.O.R.E.]	hunters	Link
2024-01-04	[Thermosash Commercial Ltd]	hunters	Link
2024-01-04	[Gunning & LaFazia, Inc.]	hunters	Link
2024-01-04	[Diablo Valley Oncology and Hematology Medical Group - Press Release]	monti	Link
2024-01-03	[Kershaw County School District]	blacksuit	Link
2024-01-03	[Bradford Health]	hunters	Link
2024-01-02	[groupe-idea.com]	lockbit3	Link
2024-01-02	[SAED International]	alphv	Link
2024-01-02	[graebener-group.com]	blackbasta	Link
2024-01-02	[leonardsexpress.com]	blackbasta	Link
2024-01-02	[nals.com]	blackbasta	Link
2024-01-02	[MPM Medical Supply]	ciphbit	Link
2024-01-01	[DELPHINUS.COM]	clop	Link
2024-01-01	[Aspiration Training]	rhysida	Link
2024-01-01	[Southeast Vermont Transit (MOOver)]	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.