Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241113

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) . . . 7
3.3 Sicherheitslücken Meldungen von Tenable . . . 11

4 Aktiv ausgenutzte Sicherheitslücken **13**
4.1 Exploits der letzten 5 Tage . . . 13
4.2 0-Days der letzten 5 Tage . . . 18

5 Die Hacks der Woche **21**
5.0.1 Sophos spielt die UNO Reverse Karte (+ Redline Stealer) . . . 21

6 Cyberangriffe: (Nov) **22**

7 Ransomware-Erpressungen: (Nov) **22**

8 Quellen **28**
8.1 Quellenverzeichnis . . . 28

9 Impressum **29**

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

Monitoring-Software Icinga: Updates schließen kritische Sicherheitslücke

In Monitoring-Software Icinga klafft eine kritische Sicherheitslücke bei der Zertifikatsüberprüfung. Updates stehen bereit, um sie zu stopfen.

- Link

—

Dell SmartFabric OS10: Angreifer können Schadcode ausführen

Dells Netzwerkbetriebssystem SmartFabric OS10 ist verwundbar. Angreifer können an mehreren Softwareschwachstellen ansetzen.

- Link

—

SAP Patchday: Acht neue Sicherheitslücken, davon eine hochriskant

Admins können etwas entspannter auf den aktuellen SAP-Patchday schauen: Von acht neuen Sicherheitslücken gilt lediglich eine als hohes Risiko.

- Link

—

Veeam Backup Enterprise Manager: Unbefugte Zugriffe durch Angreifer möglich

Ein wichtiges Sicherheitsupdate schützt Veeam Backup Enterprise Manager vor möglichen Attacken.

- Link

—

Sicherheitsupdates: Dell Enterprise SONiC für mehrere Attacken anfällig

Angreifer können sich unbefugt Zugriff auf die Netzwerkmanagementsoftware Dell Enterprise SONiC verschaffen.

- Link

—

Palo Alto untersucht mögliche Sicherheitslücke in PAN-OS-Webinterface

Palo Alto untersucht eine angebliche Codeschmuggel-Lücke in der Verwaltungsoberfläche von PAN-OS. Ein Teil betroffener Kunden wird informiert.

- Link

—

Backup-Appliance PowerProtect DD von Dell als Einfallstor für Angreifer

Die Entwickler von Dell haben in aktuellen Versionen von PowerProtect DD mehrere Sicherheitslücken geschlossen.

- Link

—

CISA warnt vor vier aktiv angegriffenen Sicherheitslücken

Die US-amerikanische IT-Sicherheitsbehörde CISA warnt davor, dass Angreifer vier Sicherheitslücken missbrauchen. Admins sollten handeln.

- Link

—

Schadcode-Attacken auf Endpoint-Management-Plattform HCL BigFix möglich

Angreifer können an mehreren Schwachstellen in HCL BigFix ansetzen und Systeme kompromittieren. Sicherheitsupdates schaffen Abhilfe.

- Link

—

Cisco: Sicherheitslücken in zahlreichen Produkten

Cisco hat für unterschiedliche Produkte Sicherheitsmitteilungen veröffentlicht. Sie behandeln auch eine kritische Schwachstelle.

- 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	0.955250000	0.994630000	Link
CVE-2023-6895	0.925010000	0.990880000	Link
CVE-2023-6553	0.949860000	0.993780000	Link
CVE-2023-6019	0.932040000	0.991580000	Link
CVE-2023-6018	0.911590000	0.989930000	Link
CVE-2023-52251	0.947690000	0.993470000	Link
CVE-2023-4966	0.970550000	0.998140000	Link
CVE-2023-49103	0.947920000	0.993500000	Link
CVE-2023-48795	0.962520000	0.995840000	Link
CVE-2023-47246	0.962070000	0.995760000	Link
CVE-2023-46805	0.962030000	0.995760000	Link
CVE-2023-46747	0.972770000	0.998930000	Link
CVE-2023-46604	0.969640000	0.997780000	Link
CVE-2023-4542	0.941060000	0.992620000	Link
CVE-2023-43208	0.974790000	0.999780000	Link
CVE-2023-43177	0.961030000	0.995560000	Link
CVE-2023-42793	0.970830000	0.998240000	Link
CVE-2023-41892	0.905460000	0.989420000	Link
CVE-2023-41265	0.920970000	0.990550000	Link
CVE-2023-38205	0.958720000	0.995200000	Link
CVE-2023-38203	0.964750000	0.996370000	Link
CVE-2023-38146	0.920950000	0.990540000	Link
CVE-2023-38035	0.974360000	0.999590000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.968430000	0.997420000	Link
CVE-2023-3519	0.965540000	0.996620000	Link
CVE-2023-35082	0.963840000	0.996150000	Link
CVE-2023-35078	0.967840000	0.997260000	Link
CVE-2023-34993	0.973050000	0.999020000	Link
CVE-2023-34634	0.926130000	0.990980000	Link
CVE-2023-34362	0.969380000	0.997710000	Link
CVE-2023-34039	0.935360000	0.991970000	Link
CVE-2023-3368	0.930810000	0.991480000	Link
CVE-2023-33246	0.973040000	0.999010000	Link
CVE-2023-32315	0.973320000	0.999140000	Link
CVE-2023-32235	0.910390000	0.989810000	Link
CVE-2023-30625	0.953680000	0.994350000	Link
CVE-2023-30013	0.966660000	0.996910000	Link
CVE-2023-29300	0.967820000	0.997250000	Link
CVE-2023-29298	0.968380000	0.997420000	Link
CVE-2023-28432	0.906870000	0.989550000	Link
CVE-2023-28343	0.962760000	0.995900000	Link
CVE-2023-28121	0.927310000	0.991100000	Link
CVE-2023-27524	0.970490000	0.998110000	Link
CVE-2023-27372	0.973760000	0.999350000	Link
CVE-2023-27350	0.969220000	0.997650000	Link
CVE-2023-26469	0.958860000	0.995220000	Link
CVE-2023-26360	0.962010000	0.995750000	Link
CVE-2023-26035	0.969120000	0.997620000	Link
CVE-2023-25717	0.950620000	0.993870000	Link
CVE-2023-25194	0.967670000	0.997200000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.961940000	0.995730000	Link
CVE-2023-24489	0.972890000	0.998960000	Link
CVE-2023-23752	0.949040000	0.993650000	Link
CVE-2023-23397	0.902750000	0.989290000	Link
CVE-2023-23333	0.963300000	0.996030000	Link
CVE-2023-22527	0.970570000	0.998150000	Link
CVE-2023-22518	0.963120000	0.995990000	Link
CVE-2023-22515	0.973100000	0.999040000	Link
CVE-2023-21839	0.933960000	0.991820000	Link
CVE-2023-21554	0.955110000	0.994590000	Link
CVE-2023-20887	0.970370000	0.998060000	Link
CVE-2023-1698	0.916400000	0.990180000	Link
CVE-2023-1671	0.962610000	0.995850000	Link
CVE-2023-0669	0.971930000	0.998600000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 12 Nov 2024

[UPDATE] [hoch] VMware Tanzu Spring Security: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in VMware Tanzu Spring Security ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Tue, 12 Nov 2024

[NEU] [hoch] Zoom Video Communications Rooms: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Zoom Video Communications Rooms und Zoom Video Communications Workplace ausnutzen, um erhöhte Berechtigungen zu erlangen, einen Denial-of-Service-Zustand zu erzeugen und vertrauliche Informationen offenzulegen.

- Link

—

Tue, 12 Nov 2024

[UPDATE] [hoch] bluez: Schwachstelle ermöglicht Codeausführung

Ein Angreifer in Funk-Reichweite kann eine Schwachstelle in bluez ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Tue, 12 Nov 2024

[UPDATE] [hoch] SMTP Implementierungen: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen SMTP Implementierungen ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Tue, 12 Nov 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

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

- Link

—

Tue, 12 Nov 2024

[UPDATE] [hoch] GNU Emacs: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in GNU Emacs ausnutzen, um beliebigen Programmcode auszuführen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Tue, 12 Nov 2024

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

Ein lokaler Angreifer kann eine Schwachstelle in QEMU ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Tue, 12 Nov 2024

[UPDATE] [hoch] FreeRDP: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein Angreifer kann mehrere Schwachstellen in FreeRDP ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Tue, 12 Nov 2024

[UPDATE] [hoch] FreeRDP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in FreeRDP ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Tue, 12 Nov 2024

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

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in verschiedenen Komponenten von Red Hat Enterprise Linux ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand auszulösen.

- Link

—

Tue, 12 Nov 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um Sicherheitsvorkehrungen zu umgehen und um Dateien zu manipulieren.

- Link

—

Tue, 12 Nov 2024

[UPDATE] [hoch] Red Hat Ansible Automation Platform: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat Ansible Automation Platform ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand erzeugen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder Cross-Site-Scripting (XSS)-Angriffe durchzuführen.

- Link

—

Tue, 12 Nov 2024

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

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen oder Daten zu manipulieren.

- Link

—

Tue, 12 Nov 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im RADIUS Protokoll ausnutzen, um Sicherheitsvorkeh-

rungen zu umgehen.
- Link

—

Tue, 12 Nov 2024

[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.
- Link

—

Tue, 12 Nov 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

—

Tue, 12 Nov 2024

[UPDATE] [hoch] Red Hat OpenShift: Schwachstelle ermöglicht Cross-Site Scripting

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat OpenShift ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen.
- Link

—

Tue, 12 Nov 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder einen ‘Denial of Service’-Zustand zu verursachen.
- Link

—

Tue, 12 Nov 2024

[NEU] [hoch] SAP Patchday November 2024: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in SAP Software ausnutzen, um seine Privilegien zu erhöhen, vertrauliche Informationen preiszugeben, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu erzeugen, einen Cross-Site-Scripting-Angriff durchzuführen und beliebigen Code auszuführen.
- Link

—

Tue, 12 Nov 2024

[UPDATE] [hoch] libarchive: Schwachstelle ermöglicht Codeausführung

Ein Angreifer kann eine Schwachstelle in libarchive ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
11/12/2024	[RHEL 9 : grafana (RHSA-2024:9115)]	critical
11/12/2024	[RHEL 9 : grafana (RHSA-2024:9473)]	critical
11/12/2024	[KB5046612: Windows 10 Version 1607 / Windows Server 2016 Security Update (November 2024)]	critical
11/12/2024	[KB5046617: Windows 11 Version 24H2 / Windows Server 2025 Security Update (November 2024)]	critical
11/12/2024	[KB5046618: Windows 11 version 22H2 / Windows Server version 23H2 Security Update (November 2024)]	critical
11/12/2024	[KB5046697: Windows Server 2012 Security Update (November 2024)]	critical
11/12/2024	[KB5046615: Windows 10 version 1809 / Windows Server 2019 Security Update (November 2024)]	critical
11/12/2024	[KB5046682: Windows Server 2012 R2 Security Update (November 2024)]	critical
11/12/2024	[KB5046616: Windows Server 2022 / Azure Stack HCI 22H2 Security Update (November 2024)]	critical
11/12/2024	[Security Update for Microsoft .NET Core SDK (November 2024)]	critical
11/12/2024	[Ubuntu 24.10 : .NET vulnerabilities (USN-7105-1)]	critical
11/12/2024	[RHEL 9 : jose (RHSA-2024:9181)]	high
11/12/2024	[RHEL 9 : gtk3 (RHSA-2024:9184)]	high

Datum	Schwachstelle	Bewertung
11/12/2024	[RHEL 9 : cups (RHSA-2024:9470)]	high
11/12/2024	[RHEL 9 : python3.11 (RHSA-2024:9450)]	high
11/12/2024	[RHEL 9 : grafana-pcp (RHSA-2024:9472)]	high
11/12/2024	[Adobe After Effects < 24.6.3 Multiple Vulnerabilities (APSB24-85)]	high
11/12/2024	[Adobe After Effects < 24.6.3 Multiple Vulnerabilities (APSB24-85) (macOS)]	high
11/12/2024	[KB5046705: Windows Server 2008 R2 Security Update (November 2024)]	high
11/12/2024	[Security Updates for Microsoft Office Online Server (November 2024)]	high
11/12/2024	[Security Updates for Microsoft Excel Products (November 2024)]	high
11/12/2024	[KB5046633: Windows 11 version 22H2 Security Update (November 2024)]	high
11/12/2024	[KB5046613: Windows 10 version 21H2 / Windows 10 Version 22H2 Security Update (November 2024)]	high
11/12/2024	[Security Updates for Microsoft Office Products (November 2024)]	high
11/12/2024	[Security Updates for Microsoft Word Products (November 2024)]	high
11/12/2024	[KB5046665: Windows 10 LTS 1507 Security Update (November 2024)]	high
11/12/2024	[Microsoft PC Manager Elevation of Privilege (November 2024)]	high
11/12/2024	[KB5046639: Windows Server 2008 Security Update (November 2024)]	high
11/12/2024	[Security Updates for Microsoft Office Products (November 2024) (macOS)]	high
11/12/2024	[Fortinet FortiClient Named Pipes Improper Access Control (FG-IR-24-199)]	high

Datum	Schwachstelle	Bewertung
11/12/2024	[Fortinet Fortigate - SSLVPN session hijacking using SAML authentication (FG-IR-23-475)]	high
11/12/2024	[Fortinet FortiClient - Missing signature verification (FG-IR-24-022) (macOS)]	high
11/12/2024	[Fortinet FortiClient Privilege escalation via lua auto patch function (FG-IR-24-144)]	high
11/12/2024	[Fortinet FortiClient Online Installer DLL Hijacking (FG-IR-24-205)]	high
11/12/2024	[Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2024-12814)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Mon, 11 Nov 2024

HASOMED Elefant / Elefant Software Updater Data Exposure / Privilege Escalation

HASOMED Elefant versions prior to 24.04.00 and Elefant Software Updater versions prior to 1.4.2.1811 suffer from having an unprotected exposed firebird database, unprotected FHIR API, multiple local privilege escalation, and hardcoded service password vulnerabilities.

- Link

—

” “Mon, 11 Nov 2024

WSO2 4.0.0 / 4.1.0 / 4.2.0 Shell Upload

WS02 versions 4.0.0, 4.1.0, and 4.2.0 are susceptible to remote code execution via an arbitrary file upload vulnerability.

- Link

—

” “Thu, 07 Nov 2024

WordPress Meetup 0.1 Authentication Bypass

WordPress Meetup plugin versions 0.1 and below suffer from an authentication bypass vulnerability.

- Link

—

” “Thu, 07 Nov 2024

CyberPanel upgrademysqlstatus Arbitrary Command Execution

Proof of concept remote command execution exploit for CyberPanel versions prior to 5b08cd6.

- Link

—

” “Thu, 07 Nov 2024

TestRail CLI FieldsParser eval Injection

While parsing test result XML files with the TestRail CLI, the presence of certain TestRail-specific fields can cause untrusted data to flow into an eval() statement, leading to arbitrary code execution. In order to exploit this, an attacker would need to be able to cause the TestRail CLI to parse a malicious XML file. Normally an attacker with this level of control would already have other avenues of gaining code execution.

- Link

—

” “Tue, 05 Nov 2024

ABB Cylon Aspect 3.08.00 Off-By-One

A vulnerability was identified in a ABB Cylon Aspect version 3.08.00 where an off-by-one error in array access could lead to undefined behavior and potential denial of service. The issue arises in a loop that iterates over an array using a less than or equals to condition, allowing access to an out-of-bounds index. This can trigger errors or unexpected behavior when processing data, potentially crashing the application. Successful exploitation of this vulnerability can lead to a crash or disruption of service, especially if the script handles large data sets.

- Link

—

” “Mon, 04 Nov 2024

Sysax Multi Server 6.99 SSH Denial Of Service

Sysax Multi Server version 6.9.9 suffers from an SSH related denial of service vulnerability.

- Link

—

” “Mon, 04 Nov 2024

Sysax Multi Server 6.99 Cross Site Scripting

Sysax Multi Server version 6.9.9 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 04 Nov 2024

IBM Security Verify Access 32 Vulnerabilities

IBM Security Verify Access versions prior to 10.0.8 suffer from authentication bypass, reuse of private keys, local privilege escalation, weak settings, outdated libraries, missing password, hardcoded se-

crets, remote code execution, missing authentication, null pointer dereference, and lack of privilege separation vulnerabilities.

- Link

—

” “Mon, 04 Nov 2024

IBM Security Verify Access Appliance Insecure Transit / Hardcoded Passwords

IBM Security Verify Access Appliance suffers from multiple insecure transit vulnerabilities, hardcoded passwords, and uninitialized variables. ibmsecurity versions prior to 2024.4.5 are affected.

- Link

—

” “Mon, 04 Nov 2024

ESET NOD32 Antivirus 18.0.12.0 Unquoted Service Path

ESET NOD32 Antivirus version 18.0.12.0 suffers from an unquoted service path vulnerability.

- Link

—

” “Mon, 04 Nov 2024

SQLite3 generate_series Stack Buffer Underflow

SQLite3 suffers from a stack buffer underflow condition in seriesBestIndex in the generate_series extension.

- Link

—

” “Mon, 04 Nov 2024

Linux khugepaged Race Conditions

khugepaged in Linux races with rmap-based zap, races with GUP-fast, and fails to call MMU notifiers.

- Link

—

” “Fri, 01 Nov 2024

Ping Identity PingIDM 7.5.0 Query Filter Injection

Ping Identity PingIDM versions 7.0.0 through 7.5.0 enabled an attacker with read access to the User collection, to abuse API query filters in order to obtain managed and/or internal user’s passwords in either plaintext or encrypted variants, based on configuration. The API clearly prevents the password in either plaintext or encrypted to be retrieved by any other means, as this field is set as protected under the User object. However, by injecting a malicious query filter, using password as the field to be filtered, an attacker can perform a blind brute-force on any victim’s user password details (encrypted object or plaintext string).

- Link

—

” “Fri, 01 Nov 2024

ABB Cylon Aspect 3.08.01 File Upload MD5 Checksum Bypass

ABB Cylon Aspect version 3.08.01 has a vulnerability in caldavInstall.php, caldavInstallAgendav.php, and caldavUpload.php files, where the presence of an EXPERTMODE parameter activates a badassMode feature. This mode allows an unauthenticated attacker to bypass MD5 checksum validation during file uploads. By enabling badassMode and setting the skipChecksum parameter, the system skips integrity verification, allowing attackers to upload or install altered CalDAV zip files without authentication. This vulnerability permits unauthorized file modifications, potentially exposing the system to tampering or malicious uploads.

- Link

—

” “Fri, 01 Nov 2024

Packet Storm New Exploits For October, 2024

This archive contains all of the 128 exploits added to Packet Storm in October, 2024.

- Link

—

” “Fri, 01 Nov 2024

SmartAgent 1.1.0 Remote Code Execution

SmartAgent version 1.1.0 suffers from an unauthenticated remote code execution vulnerability in youtubeInfo.php.

- Link

—

” “Fri, 01 Nov 2024

SmartAgent 1.1.0 Server-Side Request Forgery

SmartAgent version 1.1.0 suffers from a server-side request forgery vulnerability.

- Link

—

” “Fri, 01 Nov 2024

SmartAgent 1.1.0 SQL Injection

SmartAgent version 1.1.0 suffers from multiple unauthenticated remote SQL injection vulnerabilities.

- Link

—

” “Thu, 31 Oct 2024

WordPress Automatic 3.92.0 Path Traversal / Server-Side Request Forgery

WordPress Automatic plugin versions 3.92.0 and below proof of concept exploit that demonstrates path traversal and server-side request forgery vulnerabilities.

- Link

—

” “Thu, 31 Oct 2024

Qualitor 8.24 Server-Side Request Forgery

Qualitor versions 8.24 and below suffer from an unauthenticated server-side request forgery vulnerability.

- Link

—

” “Thu, 31 Oct 2024

CyberPanel Command Injection

Proof of concept exploit for a command injection vulnerability in CyberPanel. This vulnerability enables unauthenticated attackers to inject and execute arbitrary commands on vulnerable servers by sending crafted OPTIONS HTTP requests to /dns/getresetstatus and /ftp/getresetstatus endpoints, potentially leading to full system compromise. Versions prior to 1c0c6cb appear to be affected.

- Link

—

” “Thu, 31 Oct 2024

Skyhigh Client Proxy Policy Bypass

Proof of concept code for a flaw where a malicious insider can bypass the existing policy of Skyhigh Client Proxy without a valid release code.

- Link

—

” “Wed, 30 Oct 2024

WordPress WP-Automatic SQL Injection

This Metasploit module exploits an unauthenticated SQL injection vulnerability in the WordPress wp-automatic plugin versions prior to 3.92.1 to achieve remote code execution. The vulnerability allows the attacker to inject and execute arbitrary SQL commands, which can be used to create a malicious administrator account. The password for the new account is hashed using MD5. Once the administrator account is created, the attacker can upload and execute a malicious plugin, leading to full control over the WordPress site.

- Link

—

” “Wed, 30 Oct 2024

ABB Cylon Aspect 3.08.01 jsonProxy.php Username Enumeration

ABB Cylon Aspect version 3.08.01 is vulnerable to username enumeration in the jsonProxy.php endpoint. An unauthenticated attacker can interact with the UserManager servlet to enumerate valid usernames on the system. Since jsonProxy.php proxies requests to internal services without requiring authentication, attackers can gain unauthorized insights into valid usernames.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Tue, 12 Nov 2024
ZDI-24-1486: (0Day) G DATA Total Security Incorrect Permission Assignment Local Privilege Escalation Vulnerability
- Link
—
” “Tue, 12 Nov 2024
ZDI-24-1485: (0Day) Trimble SketchUp Viewer SKP File Parsing Memory Corruption Remote Code Execution Vulnerability
- Link
—
” “Tue, 12 Nov 2024
ZDI-24-1484: (0Day) Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability
- Link
—
” “Tue, 12 Nov 2024
ZDI-24-1483: (0Day) Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability
- Link
—
” “Tue, 12 Nov 2024
ZDI-24-1482: (0Day) Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability
- Link
—
” “Tue, 12 Nov 2024
ZDI-24-1481: (0Day) Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability
- Link
—
” “Tue, 12 Nov 2024
ZDI-24-1480: (0Day) Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability
- Link
—
” “Tue, 12 Nov 2024

ZDI-24-1479: (0Day) Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1478: (0Day) Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1477: (0Day) Trimble SketchUp Viewer SKP File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1476: (0Day) Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1475: (0Day) Trimble SketchUp Viewer SKP File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1474: (0Day) Trimble SketchUp Pro SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1473: (0Day) Trimble SketchUp SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Nov 2024

ZDI-24-1472: Veeam Backup Enterprise Manager AuthorizeByVMwareSsoToken Improper Certificate Validation Authentication Bypass Vulnerability

- Link

—

” “Mon, 11 Nov 2024

ZDI-24-1471: Panda Security Dome PSANHost Link Following Local Privilege Escalation Vulnerability

- Link

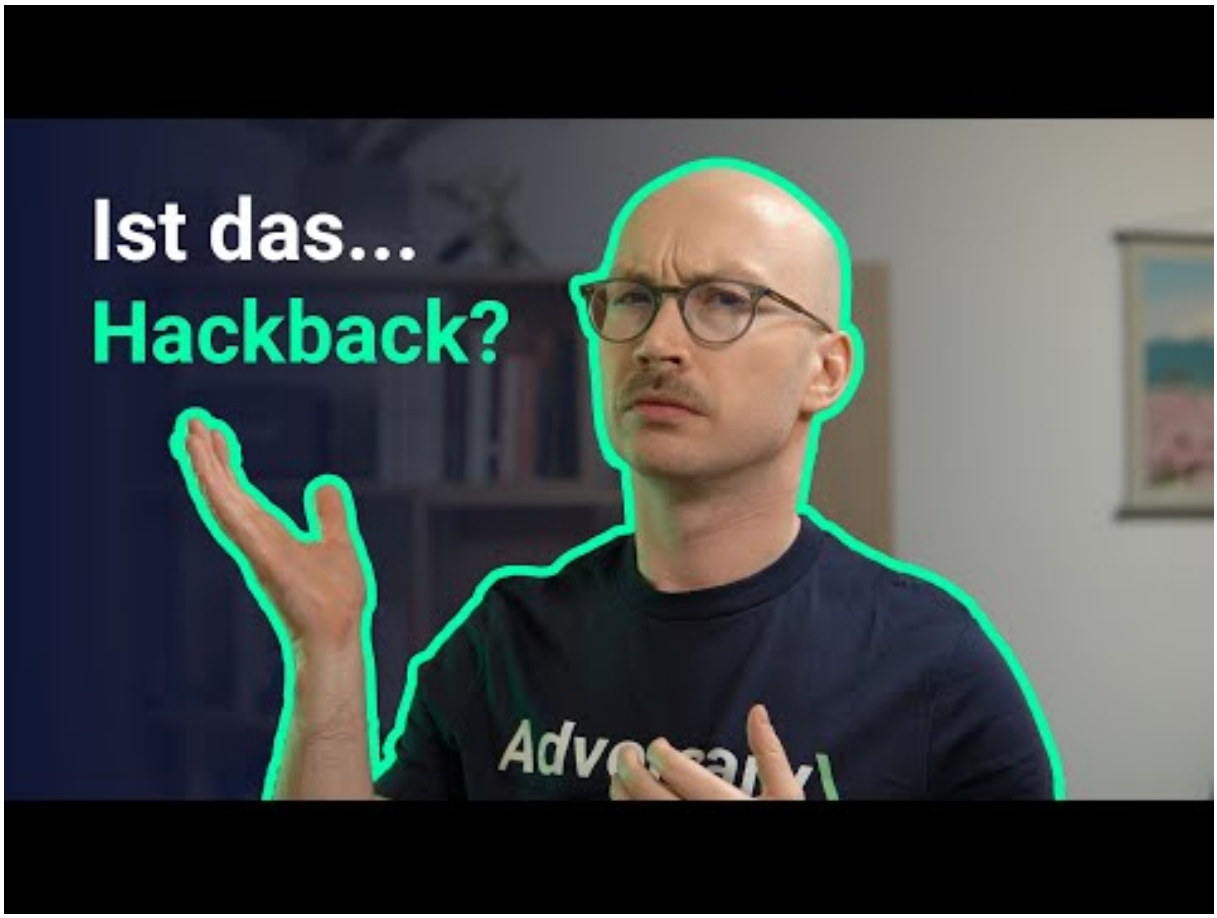
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Sophos spielt die UNO Reverse Karte (+ Redline Stealer)



Zum Youtube Video

6 Cyberangriffe: (Nov)

Datum	Opfer	Land	Information
2024-11-09	Sheboygan	[USA]	Link
2024-11-09	Berufsförderungswerk Oberhausen	[DEU]	Link
2024-11-09	Southern Oregon Veterinary Specialty Center (SOVSC)	[USA]	Link
2024-11-07	Département des Hautes-Pyrénées	[FRA]	Link
2024-11-07	Ahold Delhaize	[USA]	Link
2024-11-05	Lojas Marisa	[BRA]	Link
2024-11-05	Wexford County	[USA]	Link
2024-11-05	Ridgewood Schools	[USA]	Link
2024-11-04	Avis de Torino	[ITA]	Link
2024-11-03	Washington state courts	[USA]	Link
2024-11-03	La Sauvegarde	[FRA]	Link
2024-11-02	Memorial Hospital and Manor	[USA]	Link
2024-11-02	Kumla kommun	[SWE]	Link
2024-11-01	South East Technological University (SETU)	[IRL]	Link

7 Ransomware-Erpressungen: (Nov)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-11-13	[Value Dental Center]	everest	Link
2024-11-13	[Artistic Family Dental]	everest	Link
2024-11-13	[Asaro Dental Aesthetics]	everest	Link
2024-11-13	[Axpr Valve Science]	killsec	Link
2024-11-12	[American Associated Pharmacies]	embargo	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-11-12	[Giggle Finance]	killsec	Link
2024-11-12	[Orange County Pathology Medical Group]	raworld	Link
2024-11-12	[SK Gas]	raworld	Link
2024-11-03	[Medigroup.ca]	ransomhub	Link
2024-11-12	[steppingstonesd.org]	blacksuit	Link
2024-11-12	[Hillandale Farms]	akira	Link
2024-11-12	[jst.es]	blacksuit	Link
2024-11-12	[jarrellimc.com]	blacksuit	Link
2024-11-06	[Banco de Fomento Internacional]	lynx	Link
2024-11-11	[TaxPros of Clermont]	lynx	Link
2024-11-11	[National Institute of Administration]	killsec	Link
2024-11-07	[DSZ]	lynx	Link
2024-11-07	[Future Metals]	lynx	Link
2024-11-07	[Plowman Craven]	lynx	Link
2024-11-11	[Supply Technologies]	blacksuit	Link
2024-11-11	[Maxxis International]	blacksuit	Link
2024-11-11	[potteau.be]	ransomhub	Link
2024-11-11	[Followmont TransportPty Ltd]	akira	Link
2024-11-11	[dezinecorp.com]	blacksuit	Link
2024-11-11	[Amourgis & Associates]	hunters	Link
2024-11-11	[Dietzgen Corporation]	hunters	Link
2024-11-01	[nynewspapers.com]	ransomhub	Link
2024-11-11	[comarchs.com]	ransomhub	Link
2024-11-11	[tolbertlegal.com]	ransomhub	Link
2024-11-10	[Banco Sucredito Regional S.A.U.]	hunters	Link
2024-11-10	[OxyHealth]	killsec	Link
2024-11-10	[Immuno Laboratories, Inc]	bianlian	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-11-05	[bitquail.com]	ransomhub	Link
2024-11-09	[ATSG, Inc]	bianlian	Link
2024-11-09	[Mizuno (USA)]	bianlian	Link
2024-11-09	[Palmisano & Goodman, P.A.]	bianlian	Link
2024-11-09	[Finger Beton Unternehmensgruppe]	meow	Link
2024-11-09	[Karman Inc]	meow	Link
2024-11-09	[Siltech (siltechcorp.local)]	lynx	Link
2024-11-09	[emefarmario.com.br]	apt73	Link
2024-11-09	[Granite School District]	rhysida	Link
2024-11-09	[WimCoCorp]	lynx	Link
2024-11-09	[NEBRASKALAND]	lynx	Link
2024-11-08	[MENZIES CNAC (Jardine Aviation Services, Agility)]	spacebears	Link
2024-11-08	[bartleycorp.com]	ransomhub	Link
2024-11-08	[interlabel.be]	ransomhub	Link
2024-11-07	[del-electric.com]	ransomhub	Link
2024-11-08	[liftkits4less.com]	apt73	Link
2024-11-08	[www.lamaisonducitron.com]	apt73	Link
2024-11-08	[www.baldinger-ag.ch]	apt73	Link
2024-11-07	[Marisa S.A]	medusa	Link
2024-11-08	[www.assurified.com]	apt73	Link
2024-11-08	[www.botiga.com.uy]	apt73	Link
2024-11-08	[Healthcare Management Systems]	bianlian	Link
2024-11-08	[MedElite Group]	everest	Link
2024-11-07	[nelconinc.biz]	ransomhub	Link
2024-11-07	[www.fdc.ie]	ransomhub	Link
2024-11-07	[www.cenergica.com]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-11-07	[www.bluco.com]	ransomhub	Link
2024-11-07	[naj.ae]	darkvault	Link
2024-11-07	[Equator Worldwide]	meow	Link
2024-11-07	[Lexco]	meow	Link
2024-11-07	[europe-qualité]	incransom	Link
2024-11-07	[Winnebago Public School Foundation]	interlock	Link
2024-11-05	[Alliance Technical Group]	medusa	Link
2024-11-06	[Jomar Electrical Contractors]	medusa	Link
2024-11-06	[Howell Electric Inc]	medusa	Link
2024-11-06	[www.msdl.ca]	ransomhub	Link
2024-11-07	[Postcard Mania]	play	Link
2024-11-07	[New Law]	hunters	Link
2024-11-06	[klinkamkurpark]	helldown	Link
2024-11-06	[AMERICANVENTURE]	helldown	Link
2024-11-06	[CSIKBS]	helldown	Link
2024-11-06	[SANJACINTOCOUNY]	helldown	Link
2024-11-06	[brandenburgerplumbing.com]	ransomhub	Link
2024-11-06	[arcoexc.com]	ransomhub	Link
2024-11-06	[Lincoln University]	meow	Link
2024-11-06	[Cape Cod Regional Technical High School (capetech.us)]	fog	Link
2024-11-06	[GSR Andrade Architects (gsr-andrade.com)]	fog	Link
2024-11-05	[metroelectric.com]	ransomhub	Link
2024-11-05	[sector5.ro]	ransomhub	Link
2024-11-05	[Paragon Plastics]	play	Link
2024-11-05	[Delfin Design & Manufacturing]	play	Link
2024-11-05	[Smitty’s Supply]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-11-05	[S & W Kitchens]	play	Link
2024-11-05	[Dome Construction]	play	Link
2024-11-06	[Interoute agency]	lynx	Link
2024-11-06	[LmayInteroute agency]	lynx	Link
2024-11-05	[pacificglazing.com]	ransomhub	Link
2024-11-05	[nwhealthporter.com]	ransomhub	Link
2024-11-05	[wexfordcounty.org]	embargo	Link
2024-11-05	[ebrso]	qilin	Link
2024-11-05	[Model Die & Mold]	lynx	Link
2024-11-04	[mh-m.org]	embargo	Link
2024-11-05	[Falco Sult]	bianlian	Link
2024-11-05	[apoyoconsultoria.com]	ransomhub	Link
2024-11-05	[Webb Institute]	incransom	Link
2024-11-05	[Fylde Coast Academy Trust]	rhysida	Link
2024-11-04	[sundt.com]	ransomhub	Link
2024-11-04	[Memorial Hospital & Manor]	embargo	Link
2024-11-02	[Scolari]	dragonforce	Link
2024-11-05	[McMillan Electric Company]	medusa	Link
2024-11-04	[maxdata.com.br]	ransomhub	Link
2024-11-04	[goodline.com.au]	ransomhub	Link
2024-11-04	[kenanasugarcompany.com]	ransomhub	Link
2024-11-04	[www.schweiker.de]	ransomhub	Link
2024-11-04	[www.drbutlerandassociates.com]	ransomhub	Link
2024-11-04	[www.mssupply.com]	ransomhub	Link
2024-11-04	[fullfordelectric.com]	ransomhub	Link
2024-11-04	[College of Business - Tanzania]	hellcat	Link
2024-11-04	[Ministry of Education - Jordan]	hellcat	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-11-04	[Schneider Electric - France]	hellcat	Link
2024-11-04	[International University of Sarajevo]	medusa	Link
2024-11-04	[Whitaker Construction Group]	medusa	Link
2024-11-04	[European External Action Service (EEAS)]	hunters	Link
2024-11-04	[csucontracting.com]	ransomhub	Link
2024-11-04	[redphoenixconstruction.com]	ransomhub	Link
2024-11-04	[Air Specialists Heating & Air Conditioning]	hunters	Link
2024-11-03	[krigerconstruction.com]	ransomhub	Link
2024-11-03	[caseconstruction.com]	ransomhub	Link
2024-11-03	[lambertstonecommercial.com]	ransomhub	Link
2024-11-04	[Doctor 24x7]	killsec	Link
2024-11-03	[Hemubo]	hunters	Link
2024-11-03	[Elad municipality]	handala	Link
2024-11-03	[Russell Law Firm, LLC]	bianlian	Link
2024-11-03	[L & B Transport, L.L.C.]	bianlian	Link
2024-11-03	[guardianhc]	stormous	Link
2024-11-02	[bravodigitaltrader.co.uk]	ransomhub	Link
2024-11-02	[SVP Worldwide]	blacksuit	Link
2024-11-02	[Sumitomo]	killsec	Link
2024-11-01	[DieTech North America]	qilin	Link
2024-11-01	[www.fatboysfleetandauto.com]	ransomhub	Link
2024-11-01	[lighthouseelectric.com]	ransomhub	Link
2024-11-01	[JS McCarthy Printers]	play	Link
2024-11-01	[CGR Technologies]	play	Link
2024-11-01	[lumiplan.com]	cactus	Link
2024-11-01	[United Sleep Diagnostics]	medusa	Link
2024-11-01	[eap.gr]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-11-01	[vikurverk.is]	lockbit3	Link
2024-11-01	[mirandaproduce.com.ve]	lockbit3	Link
2024-11-01	[Cerp Bretagne Nord]	hunters	Link
2024-11-01	[Hope Valley Recovery]	rhysida	Link
2024-11-01	[lsst.ac]	cactus	Link
2024-11-01	[MCNA Dental]	everest	Link
2024-11-01	[Arctrade]	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.