Cybersecurity Morgenreport

Ausgabe: 20230914

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

Security-News

Heise - Security-Alert

Sicherheitsupdates: Schadcode-Schlupflöcher in Foxit PDF geschlossen
Angreifer können Windows-Systeme mit Foxit PDF Editor oder Foxit PDF Reader attackieren.
- Link

—

Notfallpatch sichert Firefox und Thunderbird gegen Attacken ab
Mozilla hat in seinen Webbrowsern und seinem Mailclient eine Sicherheitslücke geschlossen, die Angreifer bereits ausnutzen.
- Link

—

Patchday: Angriffe mittels präparierter PDF-Dateien auf Adobe Acrobat
Adobe hat in Acrobat und Reader, Connect und Experience Manager mehrere Sicherheitslücken geschlossen.
- Link

—

Patchday: Angreifer attackieren unter anderem Microsoft Word
Microsoft hat für Windows & Co. wichtige Sicherheitsupdates veröffentlicht. Zwei Lücken nutzen Angreifer bereits aus.
- Link

—

Patchday: SAP schließt kritische Datenleak-Lücke in BusinessObjects
Es sind wichtige Sicherheitsupdates für SAP-Software erschienen. Admins sollten zeitnah handeln.
- Link

—

Jetzt patchen! Attacken auf kritische Schadcode-Lücke in Chrome naheliegend
Google warnt vor Exploitcode für eine Schwachstelle in Chrome. Eine abgesicherte Version des Webbrowsers ist verfügbar.
- Link

—

HPE OneView: Kritische Lücke erlaubt Umgehung von Authentifizierung
HPE warnt vor mehreren Sicherheitslücken in OneView, einer Infrastrukturverwaltungssoftware. Angreifer könnten etwa die Anmeldung umgehen.
- Link

—

Sicherheitslücken: Notepad++ gegen Schadcode-Attacken abgesichert
In der aktuellen Version des freien Texteditors für Windows hat der Entwickler mehrere Sicherheitsprobleme gelöst.
- Link

—

NSO-Group-Angriff: Notfall-Updates für iPhone, iPad, Mac und Apple Watch
Apple hat am Donnerstagabend nochmals Updates für seine aktuellen Betriebssysteme nachgeschoben. Enthalten sind Fixes für einen aktiven Exploit.
- Link

—

Aruba-Controller und -Gateways mit hochriskanten Sicherheitslücken
Für Aruba-Controller und -Gateways der Serien 9000 und 9200 gibt es Updates, die hochriskante Sicherheitslücken schließen.
- Link

—

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.

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.

CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-39143	0.921370000	0.985840000	Link
CVE-2023-38035	0.960130000	0.992570000	Link
CVE-2023-3519	0.911990000	0.984960000	Link
CVE-2023-35078	0.965240000	0.994270000	Link
CVE-2023-34362	0.936790000	0.987870000	Link
CVE-2023-33246	0.971460000	0.997030000	Link
CVE-2023-32315	0.973180000	0.998100000	Link
CVE-2023-28771	0.926550000	0.986460000	Link
CVE-2023-28121	0.937820000	0.988000000	Link
CVE-2023-27524	0.964400000	0.993910000	Link
CVE-2023-27372	0.970960000	0.996760000	Link
CVE-2023-27350	0.970860000	0.996710000	Link
CVE-2023-26469	0.910820000	0.984830000	Link
CVE-2023-26360	0.904380000	0.984200000	Link
CVE-2023-25717	0.965660000	0.994490000	Link
CVE-2023-25194	0.924830000	0.986220000	Link
CVE-2023-24489	0.974410000	0.999140000	Link
CVE-2023-21839	0.960800000	0.992750000	Link
CVE-2023-21823	0.907830000	0.984530000	Link
CVE-2023-21554	0.954850000	0.991320000	Link
CVE-2023-20887	0.954150000	0.991120000	Link
CVE-2023-0669	0.965780000	0.994520000	Link

BSI - Warn- und Informationsdienst (WID)

Wed, 13 Sep 2023
[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation
Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Wed, 13 Sep 2023
[UPDATE] [hoch] Google Chrome: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 13 Sep 2023

[NEU] [hoch] Mozilla Firefox: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 13 Sep 2023

[NEU] [hoch] Adobe Acrobat und Reader: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Adobe Acrobat DC, Adobe Acrobat Reader DC, Adobe Acrobat und Adobe Acrobat Reader ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 13 Sep 2023

[NEU] [hoch] Lenovo XClarity: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein entfernter authentifizierter Angreifer kann mehrere Schwachstellen in Lenovo XClarity ausnutzen, um seine Privilegien zu erhöhen oder vertrauliche Informationen offenzulegen.

- Link

—

Wed, 13 Sep 2023

[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen ermöglichen HTTP Response Splitting

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um einen Response Splitting Angriff durchzuführen.

- Link

—

Wed, 13 Sep 2023

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial of Service Zustand herbeizuführen, Informationen offenzulegen, Dateien zu manipulieren oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 13 Sep 2023

[UPDATE] [hoch] Foxit PDF Editor und Foxit PDF Reader: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Foxit PDF Editor und Foxit Reader ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Wed, 13 Sep 2023

[NEU] [hoch] Microsoft Developer Tools: Mehrere Schwachstellen

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in verschiedenen Microsoft Developer Tools ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.

- Link

—

Wed, 13 Sep 2023

[NEU] [hoch] Microsoft Azure: Mehrere Schwachstellen

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Microsoft Azure, Microsoft Azure DevOps Server und Microsoft Azure HDInsights ausnutzen, um seine Privilegien zu erhöhen oder beliebigen Code auszuführen.

- Link

—

Wed, 13 Sep 2023

[NEU] [hoch] Microsoft Exchange Server: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Microsoft Exchange Server ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen und Informationen falsch darzustellen.

- Link

—

Wed, 13 Sep 2023
[NEU] [hoch] Microsoft Office: Mehrere Schwachstellen
Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in verschiedenen Microsoft Office Produkten ausnutzen, um seine Privilegien zu erweitern, beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen und Informationen falsch darzustellen.
- Link
—
Wed, 13 Sep 2023
[NEU] [hoch] Microsoft Windows und Microsoft Windows Server: Mehrere Schwachstellen
Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Microsoft Windows und Microsoft Windows Server ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen und seine Rechte zu erweitern.
- Link
—
Wed, 13 Sep 2023
[NEU] [hoch] ILIAS: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in ILIAS ausnutzen, um seine Privilegien zu erhöhen, Informationen offenzulegen und einen Cross Site Scripting Angriff durchzuführen.
- Link
—
Wed, 13 Sep 2023
[NEU] [hoch] Wibu-Systems CodeMeter: Schwachstelle ermöglicht Codeausführung und Privilegienerweiterung
Ein entfernter anonymer Angreifer kann eine Schwachstelle in Wibu-Systems CodeMeter ausnutzen, um beliebigen Code auszuführen oder seine Privilegien zu erweitern.
- Link
—
Tue, 12 Sep 2023
[NEU] [hoch] SAP Patchday September 2023
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in SAP Software ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder manipulieren, einen Cross-Site-Scripting-Angriff durchzuführen, Sicherheitsvorkehrungen zu umgehen oder einen Denial of Service Zustand herbeizuführen.
- Link
—
Tue, 12 Sep 2023
[NEU] [hoch] Nagios Enterprises Nagios XI: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Nagios Enterprises Nagios XI ausnutzen, um einen Cross-Site-Scripting-Angriff zu starten oder um Daten zu manipulieren.
- Link
—
Tue, 12 Sep 2023
[UPDATE] [hoch] Nvidia Treiber: Mehrere Schwachstellen
Ein lokaler Angreifer kann mehrere Schwachstellen im Nvidia Treiber ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand auszulösen, seine Privilegien zu erweitern und Daten zu manipulieren.
- Link
—
Tue, 12 Sep 2023
[UPDATE] [hoch] Nvidia Treiber: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in Nvidia Treibern ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand zu verursachen, seine Privilegien zu erweitern und Daten zu manipulieren.
- Link
—
Tue, 12 Sep 2023
[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation
Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.
- Link
—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/13/2023	[Apache Struts 2.0.0 < 2.5.32 / 6.0.0 < 6.3.0.1 Denial of Service (S2-065)]	critical
9/13/2023	[FreeBSD : electron{24,25} – multiple vulnerabilities (773ce35b-eabb-47e0-98ca-669b2b98107a)]	critical
9/13/2023	[Amazon Linux 2 : php (ALASPHP8.0-2023-004)]	critical
9/13/2023	[Amazon Linux 2 : php (ALASPHP8.0-2023-007)]	critical
9/13/2023	[Amazon Linux 2 : php (ALASPHP8.1-2023-001)]	critical
9/13/2023	[Security Updates for Microsoft Word Products C2R Multiple Vulnerabilities (September 2023)]	high
9/13/2023	[Security Updates for Microsoft Office Products C2R Multiple Vulnerabilities (September 2023)]	high
9/13/2023	[Security Updates for Microsoft Office Online Server (September 2023)]	high
9/13/2023	[Mozilla Thunderbird < 102.15.1]	high
9/13/2023	[Mozilla Firefox < 117.0.1]	high
9/13/2023	[Mozilla Thunderbird < 115.2.2]	high
9/13/2023	[Mozilla Firefox ESR < 115.2.1]	high
9/13/2023	[Mozilla Firefox ESR < 102.15.1]	high
9/13/2023	[Mozilla Firefox ESR < 102.15.1]	high
9/13/2023	[Mozilla Thunderbird < 115.2.2]	high
9/13/2023	[Mozilla Firefox < 117.0.1]	high
9/13/2023	[Mozilla Thunderbird < 102.15.1]	high
9/13/2023	[Mozilla Firefox ESR < 115.2.1]	high
9/13/2023	[Amazon Linux 2 : gcc (ALAS-2023-2245)]	high
9/13/2023	[Amazon Linux 2 : gcc10 (ALAS-2023-2244)]	high
9/13/2023	[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS : Ghostscript vulnerabilities (USN-6364-1)]	high
9/13/2023	[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Open VM Tools vulnerability (USN-6365-1)]	high
9/13/2023	[Ubuntu 23.04 : curl vulnerability (USN-6363-1)]	high
9/13/2023	[Oracle Linux 9 : qemu-kvm (ELSA-2023-5094)]	high
9/13/2023	[Oracle Linux 9 : flac (ELSA-2023-5048)]	high
9/13/2023	[Oracle Linux 9 : dmidecode (ELSA-2023-5061)]	high
9/13/2023	[FreeBSD : electron22 – multiple vulnerabilities (3693eca5-f0d3-453c-9558-2353150495bb)]	high
9/13/2023	[Security Updates for Microsoft .NET Framework (September 2023)]	high
9/13/2023	[Amazon Linux 2 : php (ALASPHP8.0-2023-006)]	high
9/13/2023	[Oracle Linux 8 : flac (ELSA-2023-5046)]	high
9/13/2023	[Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2023-12792)]	high
9/13/2023	[Ubuntu 16.04 ESM : PostgreSQL vulnerability (USN-6366-1)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“Wed, 13 Sep 2023
Ivanti Sentry Authentication Bypass / Remote Code Execution
This Metasploit module exploits an authentication bypass in Ivanti Sentry which exposes API functionality which allows for code execution in the context of the root user.
- Link
—
” “Wed, 13 Sep 2023
PHP Shopping Cart 4.2 SQL Injection
PHP Shopping Cart version 4.2 suffers from a remote SQL injection vulnerability.
- Link
—
” “Wed, 13 Sep 2023
Fundraising Script 1.0 SQL Injection
Fundraising Script version 1.0 suffers from a remote SQL injection vulnerability.
- Link
—
” “Wed, 13 Sep 2023
Blood Bank And Donor Management System 2.2 Cross Site Scripting
Blood Bank and Donor Management System version 2.2 suffers from a persistent cross site scripting vulnerability.
- Link
—
” “Wed, 13 Sep 2023
Kleeja 1.5.4 Cross Site Scripting
Kleeja version 1.5.4 suffers from a cross site scripting vulnerability.
- Link
—
” “Wed, 13 Sep 2023
K-LOANS 1.4.5 Insecure Settings
K-LOANS version 1.4.5 suffers from an ignored default credential vulnerability.
- Link
—
” “Tue, 12 Sep 2023
Equipment Rental Script 1.0 SQL Injection
Equipment Rental Script version 1.0 suffers from a remote SQL injection vulnerability.
- Link
—
” “Tue, 12 Sep 2023
Kolifa Download CMS 1.2 HTML Injection
Kolifa Download CMS version 1.2 suffers from an html injection vulnerability.
- Link
—
” “Tue, 12 Sep 2023
KALIMATAN GMS 1.0.0 Cross Site Scripting
KALIMATAN GMS version 1.0.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Tue, 12 Sep 2023
Kylin CMS 1.3.0 SQL Injection
Kylin CMS version 1.3.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.
- Link
—
” “Tue, 12 Sep 2023
Kaledo RD CMS 1.0 SQL Injection
Kaledo RD CMS version 1.0 suffers from a remote SQL injection vulnerability.
- Link
—
” “Mon, 11 Sep 2023

WordPress Slimstat Analytics 5.0.9 Cross Site Scripting / SQL Injection
WordPress Slimstat Analytics plugin versions 5.0.9 and below suffer from cross site scripting and remote SQL injection vulnerabilities.
- Link
—
” “Mon, 11 Sep 2023
VMware vRealize Log Insight Unauthenticated Remote Code Execution
VMware vRealize Log Insights versions 8.x contain multiple vulnerabilities, such as directory traversal, broken access control, deserialization, and information disclosure. When chained together, these vulnerabilities allow a remote, unauthenticated attacker to execute arbitrary commands on the underlying operating system as the root user. This Metasploit module achieves code execution via triggering a RemotePakDownloadCommand command via the exposed thrift service after obtaining the node token by calling a GetConfigRequest thrift command. After the download, it will trigger a PakUpgradeCommand for processing the specially crafted PAK archive, which then will place the JSP payload under a certain API endpoint (pre-authenticated) location upon extraction for gaining remote code execution. Successfully tested against version 8.0.2.
- Link
—
” “Mon, 11 Sep 2023
Splunk Enterprise Account Takeover
Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14 allows low-privileged users who hold a role with edit_user capability assigned to it the ability to escalate their privileges to that of the admin user by providing specially crafted web requests.
- Link
—
” “Mon, 11 Sep 2023
Linux 6.4 Use-After-Free
The Linux 6.4 kernel suffers from a use-after-free condition due to per-VMA locks that introduce a race between page fault and MREMAP_DONTUNMAP.
- Link
—
” “Mon, 11 Sep 2023
OpenPLC Webserver 3 Denial Of Service / Buffer Overflow
A buffer overflow vulnerability in OpenPLC Runtime’s webserver version 3 allows attackers to inject malicious code, leading to an internal server error that is irrecoverable. This also disables the ability to add any new slave devices through the ”Add Slave Devices” component on the Modbus page of the application.
- Link
—
” “Mon, 11 Sep 2023
Shuttle Booking Software 1.0 SQL Injection
Shuttle Booking Software version 1.0 suffers from multiple remote SQL injection vulnerabilities.
- Link
—
” “Mon, 11 Sep 2023
Varient News Magazine Script 1.3.0 Insecure Settings
Varient News Magazine Script version 1.3.0 suffers from an ignored default credential vulnerability.
- Link
—
” “Mon, 11 Sep 2023
IWT Imagine CMS 1.0 Cross Site Scripting
IWT Imagine CMS version 1.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Mon, 11 Sep 2023
iSmile Soft CMS 0.3.0 Cross Site Scripting
iSmile Soft CMS version 0.3.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Fri, 08 Sep 2023
WinRAR Remote Code Execution
This Metasploit module exploits a vulnerability in WinRAR (CVE-2023-38831). When a user opens a crafted RAR file and its embedded document, the decoy document is executed, leading to code execution.

- Link

—

” “Fri, 08 Sep 2023

LG Simple Editor Remote Code Execution

This Metasploit module exploits broken access control and directory traversal vulnerabilities in LG Simple Editor software for gaining code execution. The vulnerabilities exist in versions of LG Simple Editor prior to v3.21. By exploiting this flaw, an attacker can upload and execute a malicious JSP payload with the SYSTEM user permissions.

- Link

—

” “Fri, 08 Sep 2023

Sonicwall GMS 9.9.9320 Remote Code Execution

This Metasploit module exploits a series of vulnerabilities - including auth bypass, SQL injection, and shell injection - to obtain remote code execution on SonicWall GMS versions 9.9.9320 and below.

- Link

—

” “Fri, 08 Sep 2023

OpenTSDB 2.4.1 Unauthenticated Command Injection

This Metasploit module exploits an unauthenticated command injection vulnerability in the key parameter in OpenTSDB through 2.4.1 in order to achieve unauthenticated remote code execution as the root user. The module first attempts to obtain the OpenTSDB version via the api. If the version is 2.4.1 or lower, the module performs additional checks to obtain the configured metrics and aggregators. It then randomly selects one metric and one aggregator and uses those to instruct the target server to plot a graph. As part of this request, the key parameter is set to the payload, which will then be executed by the target if the latter is vulnerable. This module has been successfully tested against OpenTSDB version 2.4.1.

- Link

—

” “Fri, 08 Sep 2023

Kibana Timelion Prototype Pollution Remote Code Execution

Kibana versions before 5.6.15 and 6.6.1 contain an arbitrary code execution flaw in the Timelion visualizer. An attacker with access to the Timelion application could send a request that will attempt to execute javascript code. This leads to an arbitrary command execution with permissions of the Kibana process on the host system. Exploitation will require a service or system reboot to restore normal operation. The WFSDELAY parameter is crucial for this exploit. Setting it too high will cause MANY shells (50-100+), while setting it too low will cause no shells to be obtained. WFSDELAY of 10 for a docker image caused 6 shells.

- Link

—

”

0-Day

“Tue, 12 Sep 2023

ZDI-23-1431: Foxit PDF Reader Annotation Use-After-Free Information Disclosure Vulnerability

- Link

—

” “Tue, 12 Sep 2023

ZDI-23-1430: Foxit PDF Reader Annotation Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Sep 2023

ZDI-23-1429: Foxit PDF Reader PDF File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Sep 2023

ZDI-23-1428: Foxit PDF Reader AcroForm Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 12 Sep 2023
ZDI-23-1427: Foxit PDF Reader Annotation Use-After-Free Remote Code Execution Vulnerability
- Link

—

” “Tue, 12 Sep 2023
ZDI-23-1426: Foxit PDF Reader Annotation Use-After-Free Information Disclosure Vulnerability
- Link

—

” “Tue, 12 Sep 2023
ZDI-23-1425: Foxit PDF Reader Doc Object Use-After-Free Remote Code Execution Vulnerability
- Link

—

” “Tue, 12 Sep 2023
ZDI-23-1424: Foxit PDF Reader XFA Doc Object Use-After-Free Remote Code Execution Vulnerability
- Link

—

” “Tue, 12 Sep 2023
ZDI-23-1423: Foxit PDF Reader XFA Doc Object Out-Of-Bounds Read Information Disclosure Vulnerability
- Link

—

” “Tue, 12 Sep 2023
ZDI-23-1422: Foxit PDF Reader templates Use-After-Free Information Disclosure Vulnerability
- Link

—

” “Tue, 12 Sep 2023
ZDI-23-1421: Microsoft Office Word FBX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability
- Link

—

” “Tue, 12 Sep 2023
ZDI-23-1420: Microsoft Exchange DumpDataReader Deserialization of Untrusted Data Arbitrary File Write Vulnerability
- Link

—

” “Tue, 12 Sep 2023
ZDI-23-1419: Microsoft Exchange ApprovedApplicationCollection Deserialization of Untrusted Data Remote Code Execution Vulnerability
- Link

—

” “Tue, 12 Sep 2023
ZDI-23-1418: Microsoft Exchange ProjectInstance Deserialization of Untrusted Data Information Disclosure Vulnerability
- Link

—

” “Tue, 12 Sep 2023
ZDI-23-1417: Microsoft Exchange Project Deserialization of Untrusted Data Information Disclosure Vulnerability
- Link

—

” “Tue, 12 Sep 2023
ZDI-23-1416: Microsoft 3D Builder GLB File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability
- Link

—

” “Tue, 12 Sep 2023
ZDI-23-1415: Microsoft 3D Builder WRL File Parsing Out-Of-Bounds Write Remote Code Ex-

ecution Vulnerability
- Link
—
” “Tue, 12 Sep 2023
ZDI-23-1414: Microsoft 3D Builder PLY File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability
- Link
—
” “Tue, 12 Sep 2023
ZDI-23-1413: Microsoft 3D Builder WRL File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability
- Link
—
” “Tue, 12 Sep 2023
ZDI-23-1412: Microsoft 3D Builder WRL File Parsing Memory Corruption Remote Code Execution Vulnerability
- Link
—
” “Tue, 12 Sep 2023
ZDI-23-1411: Microsoft 3D Builder PLY File Parsing Memory Corruption Remote Code Execution Vulnerability
- Link
—
” “Tue, 12 Sep 2023
ZDI-23-1410: Microsoft Windows UMPDDrvStrokePath Use-After-Free Local Privilege Escalation Vulnerability
- Link
—
” “Tue, 12 Sep 2023
ZDI-23-1409: Microsoft Windows UMPDDrvStrokeAndFillPath Use-After-Free Local Privilege Escalation Vulnerability
- Link
—
” “Tue, 12 Sep 2023
ZDI-23-1408: Microsoft Windows UMPDDrvStrokeAndFillPath Use-After-Free Local Privilege Escalation Vulnerability
- Link
—
” “Tue, 12 Sep 2023
ZDI-23-1407: Microsoft Windows UMPDDrvBitBlt Use-After-Free Local Privilege Escalation Vulnerability
- Link
—
” “Tue, 12 Sep 2023
ZDI-23-1406: Microsoft Windows UMPDDrvFillPath Use-After-Free Local Privilege Escalation Vulnerability
- Link
—
” “Tue, 12 Sep 2023
ZDI-23-1405: Microsoft Windows CLFS Out-Of-Bounds Read Information Disclosure Vulnerability
- Link
—
” “Tue, 12 Sep 2023
ZDI-23-1404: Microsoft Windows CLFS Out-Of-Bounds Read Information Disclosure Vulnerability
- Link
—
” “Tue, 12 Sep 2023
ZDI-23-1403: Microsoft Azure DevOps Server MachinePropertyBag Deserialization of Untrusted Data Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 11 Sep 2023

ZDI-23-1402: Hewlett Packard Enterprise OneView resetAdminPassword Authentication Bypass Vulnerability

- Link

—

” “Mon, 11 Sep 2023

ZDI-23-1401: ManageEngine ADManager Plus download Directory Traversal Information Disclosure Vulnerability

- Link

—

”

Die Hacks der Woche

mit Martin Haunschmid

Schlechte Neuigkeiten: LastPass Tresore geknackt? UND: Wie der Microsoft Signing Key verschwand

Zum Youtube Video

Cyberangriffe: (Sep)

Datum	Opfer	Land	Information
2023-09-12	Un prestataire de Pelmorex Corp.	[CAN]	Link
2023-09-12	Netglobalis (IFX Networks)	[CHL]	Link
2023-09-11	MGM Resorts	[USA]	Link
2023-09-11	Partenaire de moBiel	[DEU]	Link
2023-09-11	Le système d'information judiciaire régional (REJIS) du comté de St. Louis	[USA]	Link
2023-09-07	Le groupe hospitalier Saint-Vincent à Strasbourg	[FRA]	Link
2023-09-06	L'académie St Augustine à Maidstone	[GBR]	Link
2023-09-06	Comté de Hinds	[USA]	Link
2023-09-05	Mairie de Séville	[ESP]	Link
2023-09-05	Financial Services Commission (FSC)	[JAM]	Link
2023-09-05	Decatur Independent School District (DISD)	[USA]	Link
2023-09-05	Thermae 2000	[NLD]	Link
2023-09-04	Maiden Erlegh Trust	[GBR]	Link
2023-09-01	Comitato Elettrotecnico Italiano (CEI)	[ITA]	Link
2023-09-01	Secrétariat de l'environnement et des ressources naturelles (Semarnat)	[MEX]	Link

Ransomware-Erpressungen: (Sep)

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-09-13	[Enpos]	stormous	Link
2023-09-13	[clearcreek.org]	lockbit3	Link
2023-09-13	[Financial Services Commission]	blacksuit	Link
2023-09-13	[Cedar Holdings]	trigona	Link
2023-09-13	[Benefit Management INC]	knight	Link
2023-09-13	[Dpc & S]	play	Link
2023-09-13	[Carpet One]	play	Link
2023-09-13	[Markentrainer Werbeagentur, Elwema Automotive]	play	Link
2023-09-13	[Tanachira Group]	knight	Link
2023-09-12	[Accuride]	akira	Link
2023-09-12	[Abbeyfield]	incransom	Link
2023-09-12	[Morgan Smith Industries LLC]	knight	Link
2023-09-12	[Decarie Motors Inc]	knight	Link
2023-09-12	[sinloc.com]	lockbit3	Link
2023-09-12	[M-Extend / MANIP]	alphv	Link
2023-09-12	[Dee Sign]	lorenz	Link
2023-09-12	[Credifiel was hacked and a lot of personal customer and financial information was stolen]	alphv	Link
2023-09-12	[Derrimon Trading was hacked. Critical data of the company and its customers was stolen]	alphv	Link
2023-09-12	[CORTEL Technologies]	qilin	Link
2023-09-11	[Alps Alpine]	blackbyte	Link
2023-09-11	[24/7 Express Logistics (Unpay-Start Leaking)]	ragroup	Link
2023-09-07	[International Joint Commission]	noescape	Link
2023-09-02	[Altmann Dental GmbH & Co KG]	noescape	Link
2023-09-03	[AdSage Technology Co., Ltd.]	noescape	Link
2023-09-11	[deeroaks.com]	lockbit3	Link
2023-09-11	[Cmranallolaw.com]	everest	Link
2023-09-11	[Wardlaw Claims Service]	cactus	Link
2023-09-11	[Levine Bagade Han]	cactus	Link
2023-09-11	[Leekes]	cactus	Link
2023-09-11	[My Insurance Broker]	cactus	Link
2023-09-11	[Unimarketing]	cactus	Link
2023-09-11	[cfsigroup.ca]	lockbit3	Link
2023-09-11	[Wave Hill]	medusa	Link
2023-09-11	[Steripharma]	medusa	Link
2023-09-11	[co.grant.mn.us]	lockbit3	Link
2023-09-11	[KUITS Solicitors]	alphv	Link
2023-09-11	[Ford Covesa]	8base	Link
2023-09-10	[New Venture Escrow]	bianlian	Link
2023-09-10	[BOZOVICH TIMBER PRODUCTS INC]	mallox	Link
2023-09-10	[njsba.com]	abyss	Link
2023-09-10	[Singing River Health System]	rhysida	Link
2023-09-10	[Core Desktop]	rhysida	Link
2023-09-09	[Kirby Risk]	blackbyte	Link
2023-09-09	[airelec.bg]	ransomed	Link
2023-09-09	[pilini.bg]	ransomed	Link
2023-09-09	[kasida.bg]	ransomed	Link
2023-09-09	[proxy-sale.com]	ransomed	Link
2023-09-09	[IT-Center Syd]	rhysida	Link
2023-09-08	[www.northriverco.com]	abyss	Link
2023-09-08	[sd69.org]	lockbit3	Link
2023-09-08	[milbermakris.com]	lockbit3	Link
2023-09-08	[monaco-technologies.com]	lockbit3	Link
2023-09-08	[UNIVERSAL REALTY GROUP]	8base	Link
2023-09-08	[Geo Tek]	cactus	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-09-08	[hanwha.com]	lockbit3	Link
2023-09-08	[Custom Powder Systems]	cactus	Link
2023-09-08	[JSS Almonds]	cactus	Link
2023-09-08	[atWork Office Furniture]	cactus	Link
2023-09-08	[BRiC Partnership]	cactus	Link
2023-09-08	[PAUL-ALEXANDRE DOICESCO]	qilin	Link
2023-09-08	[WACOAL]	qilin	Link
2023-09-08	[Linktera]	ransomed	Link
2023-09-07	[24/7 Express Logistics]	ragroup	Link
2023-09-07	[FOCUS Business Solutions]	blackbyte	Link
2023-09-07	[Chambersburg Area School District]	blackbyte	Link
2023-09-07	[Pvc-ms]	stormous	Link
2023-09-07	[toua.net]	lockbit3	Link
2023-09-07	[Conselho Superior da Justiça do Trabalho]	8base	Link
2023-09-07	[Sebata Holdings (MICROmega Holdings)]	bianlian	Link
2023-09-07	[TORMAX USA]	cactus	Link
2023-09-07	[West Craft Manufacturing]	cactus	Link
2023-09-07	[Trimaran Capital Partners]	cactus	Link
2023-09-07	[Specialised Management Services]	cactus	Link
2023-09-06	[nobleweb.com]	lockbit3	Link
2023-09-06	[protosign.it]	lockbit3	Link
2023-09-06	[concrejato.com.br]	lockbit3	Link
2023-09-06	[meroso.be]	lockbit3	Link
2023-09-06	[qsoftnet.com]	lockbit3	Link
2023-09-06	[ragasa.com.mx]	lockbit3	Link
2023-09-06	[I Keating Furniture World]	incransom	Link
2023-09-06	[onyx-fire.com]	lockbit3	Link
2023-09-06	[gormanusa.com]	lockbit3	Link
2023-09-06	[Israel Medical Center - leaked]	ragnarlocker	Link
2023-09-06	[It4 Solutions Robras]	incransom	Link
2023-09-06	[Smead]	blackbyte	Link
2023-09-06	[Solano-Napa Pet Emergency Clinic]	knight	Link
2023-09-06	[Ayass BioScience]	alphv	Link
2023-09-06	[Sabre Corporation]	dunghill_leak	Link
2023-09-06	[Energy One]	akira	Link
2023-09-06	[FRESH TASTE PRODUCE USA AND ASSOCIATES INC.]	8base	Link
2023-09-06	[Chula Vista Electric (CVE)]	8base	Link
2023-09-05	[Precisely, Winshuttle]	play	Link
2023-09-05	[Kikkerland Design]	play	Link
2023-09-05	[Markentrainer Werbeagentur]	play	Link
2023-09-05	[Master Interiors]	play	Link
2023-09-05	[Bordelon Marine]	play	Link
2023-09-05	[Majestic Spice]	play	Link
2023-09-04	[Infinity Construction Company]	noescape	Link
2023-09-05	[Maxxd Trailers]	cactus	Link
2023-09-05	[MINEMAN Systems]	cactus	Link
2023-09-05	[Promotrans]	cactus	Link
2023-09-05	[Seymours]	cactus	Link
2023-09-02	[Strata Plan Australia FULL LEAK]	alphv	Link
2023-09-02	[TissuPath Australia FULL LEAK]	alphv	Link
2023-09-05	[Marfrig Global Foods]	cactus	Link
2023-09-05	[Brooklyn Premier Orthopedics FULL LEAK!]	alphv	Link
2023-09-05	[Barry Plant LEAK!]	alphv	Link
2023-09-05	[Barsco]	cactus	Link
2023-09-05	[Foroni SPA]	cactus	Link
2023-09-05	[Hornsyld Købmandsgaard]	cactus	Link
2023-09-05	[Lagarde Meregnani]	cactus	Link
2023-09-05	[spmblaw.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-09-05	[Unimed]	trigona	Link
2023-09-05	[Cyberport]	trigona	Link
2023-09-05	[godbeylaw.com]	lockbit3	Link
2023-09-01	[Firmdale Hotels]	play	Link
2023-09-04	[easydentalcare.us]	ransomed	Link
2023-09-04	[quantinuum.com]	ransomed	Link
2023-09-04	[laasr.eu]	ransomed	Link
2023-09-04	[medcenter-tambov.ru]	ransomed	Link
2023-09-04	[makflix.eu]	ransomed	Link
2023-09-04	[nucleus.live]	ransomed	Link
2023-09-04	[wantager.com]	ransomed	Link
2023-09-04	[Zurvita]	ragroup	Link
2023-09-04	[Piex Group]	ragroup	Link
2023-09-04	[Yuxin Automobile Co.Ltd ( )]	ragroup	Link
2023-09-02	[Mulkay Cardiology Consultants]	noescape	Link
2023-09-04	[Balcan]	cactus	Link
2023-09-04	[Barco Uniforms]	cactus	Link
2023-09-04	[Swipe.bg]	ransomed	Link
2023-09-04	[Balmit Bulgaria]	ransomed	Link
2023-09-04	[cdwg.com]	lockbit3	Link
2023-09-04	[Betton France]	medusa	Link
2023-09-04	[Jules B]	medusa	Link
2023-09-04	[VVandA]	8base	Link
2023-09-04	[Prodegest Assessors]	8base	Link
2023-09-04	[Knight Barry Title]	snatch	Link
2023-09-03	[phms.com.au]	ransomed	Link
2023-09-03	[paynesvilleareainsurance.com]	ransomed	Link
2023-09-03	[SKF.com]	ransomed	Link
2023-09-03	[gosslaw.com]	lockbit3	Link
2023-09-03	[marianoshoes.com]	lockbit3	Link
2023-09-03	[Arkopharma]	incransom	Link
2023-09-02	[Taylor University]	moneymessage	Link
2023-09-03	[Riverside Logistics]	moneymessage	Link
2023-09-03	[Estes Design & Manufacturing]	moneymessage	Link
2023-09-03	[Aiphone]	moneymessage	Link
2023-09-03	[DDB Unlimited (ddbunlimited.com)]	rancoz	Link
2023-09-03	[Rick Ramos Law (rickramoslaw.com)]	rancoz	Link
2023-09-03	[Newton Media A.S]	alphv	Link
2023-09-03	[Lawsonlundell]	alphv	Link
2023-09-02	[glprop.com]	lockbit3	Link
2023-09-02	[Strata Plan Australia]	alphv	Link
2023-09-02	[TissuPath Australia]	alphv	Link
2023-09-02	[seasonsdarlingharbour.com.au]	lockbit3	Link
2023-09-02	[nerolac.com]	lockbit3	Link
2023-09-02	[ramlowstein.com]	lockbit3	Link
2023-09-02	[Barry Plant Real Estate Australia]	alphv	Link
2023-09-02	[sterncoengineers.com]	lockbit3	Link
2023-09-02	[attorneydanwinder.com]	lockbit3	Link
2023-09-02	[designlink.us]	lockbit3	Link
2023-09-02	[gh2.com]	lockbit3	Link
2023-09-02	[DOIT - Canadian IT company allowed leak of its own clients.]	ragnarlocker	Link
2023-09-02	[SKF.com]	everest	Link
2023-09-02	[Powersportsmarketing.com]	everest	Link
2023-09-02	[Statefarm.com]	everest	Link
2023-09-02	[Aban Tether & OK exchange]	arvinclub	Link
2023-09-02	[cc-gorgesardeche.fr]	lockbit3	Link
2023-09-01	[cciamp.com]	lockbit3	Link
2023-09-01	[Templeman Consulting Group Inc]	bianlian	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-09-01	[vodatech.com.tr]	lockbit3	Link
2023-09-01	[F??????? ?????s]	play	Link
2023-09-01	[Hawaii Health System]	ransomed	Link
2023-09-01	[hamilton-techservices.com]	lockbit3	Link
2023-09-01	[aquinas.qld.edu.au]	lockbit3	Link
2023-09-01	[konkconsulting.com]	lockbit3	Link
2023-09-01	[Piex Group]	ragroup	Link
2023-09-01	[Yuxin Automobile Co.Ltd( )]	ragroup	Link

Quellen

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

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.