



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Aktive Ausnutzung einer kritischen Sicherheitslücke in Control Web Panel

CSW-Nr. 2023-196800-1032, Version 1.0, 16.01.2023

IT-Bedrohungslage*: 3 / Orange

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Am 3. Januar 2023 veröffentlichte der IT-Sicherheitsforscher Numan Türle von Gais Cyber Security einen Proof of Concept zu einer Schwachstelle in der Server-Verwaltungssoftware Control Web Panel (CWP) – ehemals CentOS Web Panel [TWI2022], [GIT2022]. Die Sicherheitslücke ermöglicht es einem entfernten, nicht authentifizierten Angreifer, auf Basis einer fehlenden Neutralisierung von Eingaben (CWE-78; [CWE2022]) Code auf dem betroffenen System auszuführen. Die Bekanntgabe der Informationen folgte auf ein abgeschlossenes Schwachstellenkoordinierungsverfahren, das Türle im vergangenen Oktober beim Hersteller angestoßen hatte.

Gemäß Common Vulnerability Scoring System ist die Schwachstelle mit einem Wert von 9.8 als „kritisch“ eingestuft (CVSSv3.1). In den Common Vulnerabilities and Exposures wird die Sicherheitslücke unter der Nummer CVE-2022-44877 [CVE2022] geführt.

Wenige Tage nach der Veröffentlichung fanden bereits Angriffsversuche auf verwundbare Systeme statt. Dabei wurden verschiedene Vorgehensweisen der Angreifenden beobachtet. Unter anderem kam es zur Installation von Shells auf den Servern, teilweise beschränkten sich die Angriffe lediglich auf die Sammlung von Informationen.

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.

2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.

3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.

4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Bewertung

Die große Verbreitung von CWP, der vorliegende Proof of Concept sowie die vergleichsweise einfache Ausnutzbarkeit der Schwachstelle führen dazu, dass die Wahrscheinlichkeit eines Cyber-Angriffs derzeit als sehr hoch eingeschätzt werden muss.

Auch wenn sich die Angreifenden zum Teil nur auf die Informationsbeschaffung beschränken, könnten die gewonnenen Erkenntnisse zur Vorbereitung späterer Angriffe genutzt werden.

Maßnahmen

Die Entwickler von Control Web Panel haben am 25. Oktober 2022 ein Update zur Verfügung gestellt, in dem die Schwachstelle geschlossen wird [CWP2022]. IT-Sicherheitsverantwortliche sollten schnellstmöglich mindestens dieses Update oder eine neuere Version (Version 0.9.8.1148) prüfen und installieren.

Gleichzeitig sollten Log-Dateien geprüft werden, um bereits erfolgte Angriffsversuche zu detektieren. Hinweise können zum Beispiel vorgenommene Veränderungen am System oder Zugriffe von verdächtigen IP-Adressen sein. Weitere Informationen zur Detektion von sicherheitsrelevanten Ereignissen finden sich im IT-Grundschutz [BSI2022].

Links

[BSI2022] DER.1 Detektion von sicherheitsrelevanten Ereignissen (Edition 2022):

<https://bsi.bund.de/dok/989184>

[CVE2022] National Vulnerability Database - CVE-2022-44877 Detail:

<https://nvd.nist.gov/vuln/detail/CVE-2022-44877>

[CWE2022] CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'):

<http://cwe.mitre.org/data/definitions/78.html>

[CWP2022] Control Web Panel Changelog:

<https://control-webpanel.com/changelog#1669855527714-450fb335-6194>

[GIT2022] Centos Web Panel 7 Unauthenticated Remote Code Execution - CVE-2022-44877:

<https://github.com/numanturle/CVE-2022-44877>

[TWI2022] Twitter-Account von Numan Türle:

<https://twitter.com/numanturle>

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

- 1) Was ist das Traffic Light Protokoll?
Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.
- 2) Welche Einstufungen existieren?
 - **TLP:CLEAR: Unbegrenzte Weitergabe**
Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.
 - **TLP:GREEN: Organisationsübergreifende Weitergabe**
Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.
 - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe
Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
 - **TLP:RED: Persönlich, nur für benannte Empfänger**
Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.
- 3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?
Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.
- 4) Was passiert, wenn ich die Einstufung nicht beachte?
Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-ingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.