



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

# Kritische Schwachstellen in BIG-IP Produkten von F5

CSW-Nr. 2022-224037-1032, Version 1.0, 09.05.2022

IT-Bedrohungslage\*: 2 / Gelb

**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:WHITE: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE 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 4. Mai 2022 veröffentlichte das Unternehmen F5 ein Security Advisory zu einer Schwachstelle, die es Angreifenden ermöglichen könnte, auf Lösungen aus der BIG-IP-Produktfamilie Befehle auszuführen, Dienste zu deaktivieren, Dateien anzulegen/zu löschen und somit letztendlich die Kontrolle über das Gerät zu erlangen [F5BIGa]. Ausschlaggebend hierfür ist eine Schwachstelle in der Authentifizierung der iControl REST Schnittstelle (CVE-2022-1388) [F5BIGb]. Die Schwachstelle wird nach Common Vulnerability Scoring System (CVSS) mit einem Wert von 9.8 als "kritisch" eingestuft (CVSSv3).

Betroffen sind Komponenten mit folgenden BIG-IP Versionen:

- 16.1.0 - 16.1.2
- 15.1.0 - 15.1.5
- 14.1.0 - 14.1.4
- 13.1.0 - 13.1.4
- 12.1.0 - 12.1.6 (Ende des regulären Supports bereits erreicht.)
- 11.6.1 - 11.6.5 (Ende des regulären Supports bereits erreicht.)

Nach der Bekanntgabe des Sachverhalts durch den Hersteller häufen sich Berichte in IT-Portalen und Sozialen Medien, wonach eine Ausnutzung der Schwachstelle als besonders einfach eingeschätzt wird. Unter

\* 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.

anderem haben Sicherheitsforschende des Unternehmens Horizon3.ai am 7. Mai 2022 angekündigt, in der aktuellen Kalenderwoche (KW 19) Proof-of-Concept-Code (PoC-Code) zur Schwachstelle zu veröffentlichen [Twi2022a]. Weitere Posts zum hier beschriebenen Sachverhalt lassen darauf schließen, dass auch von anderen Quellen zeitnah PoCs veröffentlicht werden bzw. bereits im Umlauf sind [Twi2022b], [Twi2022c].

## Bewertung

Aufgrund ihrer zentralen Bedeutung für die IT in Organisationen stellen die gefährdeten Produkte ein attraktives Ziel für Cyber-Angriffe dar. Die scheinbar triviale Ausnutzbarkeit der Schwachstellen sowie das kurze Zeitfenster zwischen Bekanntgabe des Herstellers und Veröffentlichung von PoC-, ggf. sogar Exploit-Code im Internet, erhöhen das Risiko eines erfolgreichen Angriffes signifikant.

## Maßnahmen

Das BSI empfiehlt Nutzenden der genannten Komponenten, die vom Hersteller bereitgestellten Patches kurzfristig einzuspielen. Sofern die eingesetzte BIG-IP-Version bereits nicht mehr mit Updates unterstützt wird, sollte schnellstmöglich geprüft werden, ob das Upgrade zu einer aktuellen Version möglich ist.

Weitere Hinweise zum Patch- und Änderungsmanagement befinden sich im IT-Grundschutz [BSI2022].

Falls diese Empfehlungen nicht umgesetzt werden können, zeigt F5 auf seiner Webseite zusätzliche Mitigationsmaßnahmen auf [F5BIGa]. Hierzu zählen:

- die Einrichtung von IP-basierte Zugriffskontrollen,
- das Blocken von Zugriffen auf iControl REST mithilfe des Management Interfaces sowie
- Anpassungen der BIG-IP httpd-Konfiguration.

Konkrete Umsetzungshinweise können der Veröffentlichung des Herstellers entnommen werden.

## Links

[F5BIGa] K23605346: BIG-IP iControl REST vulnerability CVE-2022-1388: <https://support.f5.com/csp/article/K23605346>

[F5BIGb] iControlRest Home: <https://clouddocs.f5.com/api/icontrol-rest/>

[Twi2022a] <https://twitter.com/Horizon3Attack/status/1522715182014902272>

[Twi2022b] <https://twitter.com/AnnaViolet20/status/1523564632140509184>

[Twi2022c] <https://twitter.com/ptswarm/status/1522873828896034816>

[BSI2022] BSI IT-Grundschutz: OPS.1.1.3:Patch- und Änderungsmanagement: <https://bsi.bund.de/dok/989196>

# 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 TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensiblen Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.
- 2) Welche Einstufungen existieren?
  - **TLP:WHITE: Unbegrenzte Weitergabe**  
Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
  - **TLP:GREEN: Organisationsübergreifende Weitergabe**  
Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
  - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**  
Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. 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. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.
- 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:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.