



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

# Kritische Schwachstellen der BIG-IP / BIG-IQ Produkte von F5

*Beobachtung erster Angriffe*

CSW-Nr. 2021-198488-1032, Version 1.0, 22.03.2021

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

Das Unternehmen F5 – Anbieter verschiedener Netzwerklösungen für Unternehmen und andere Organisationen – machte am 12. März auf mehrere BIG-IP / BIG-IQ Produkte betreffende kritische Schwachstellen aufmerksam [BIGIP2021a]. Angreifer sind demnach in der Lage, Authentifizierungen zu umgehen, aus der Ferne Befehle bzw. Code auszuführen oder DDoS-Attacken zu initiieren. Das Bundesamt für Sicherheit in der Informationstechnik hatte auf diesen Sachverhalt zeitnah über seinen Warn- und Informationsdienst [CER2021] sowie per Twitter [TWI2021] hingewiesen.

Inzwischen wurden jedoch mehrere Exploit Codes veröffentlicht und es machen Berichte über Angriffe die Runde [NCC2021], was das BSI zum Versand dieser Warnmeldung veranlasst.

Bei den Schwachstellen handelt es sich im Detail um:

- **CVE-2021-22986: Eine Remote-Command-Execution Schwachstelle im iControl REST Interface, die keine Authentifizierung erfordert [BIGIP2021b].**
- CVE-2021-22987 bis CVE-2021-22990: Angriffe auf das Traffic User Interface (TMUI), wodurch ebenfalls Befehle aus der Ferne ausgeführt werden können. Teilweise wird hierfür der Betrieb im Appliance Mode vorausgesetzt [BIGIP2021c], [BIGIP2021d], [BIGIP2021e], [BIGIP2021f].

\* 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.

- **CVE-2021-22991: Der Traffic Management Microkernel (TMM) kann genutzt werden, um einen Buffer Overflow bzw. eine daraus resultierende DDoS-Attacke zu erzeugen. Gleichzeitig ist bei ausgewählten Konfigurationen die Umgehung der Authentifizierungsmechanismen und in der Folge die Ausführung von Code aus der Ferne möglich [BIGIP2021g].**
- CVE-2021-22992: Eine schadhafte HTTP-Response an die Produkte Advanced Web Application Firewall (WAF) bzw. BIG-IP Application Security Manager (ASM) kann ebenfalls in einem DDoS-Angriff enden. Auch hier gibt der Hersteller an, dass grundsätzlich Remote Code Execution bzw. eine vollständige Kompromittierung des Systems denkbar sind – sofern der Angreifer bereits andere Teile des Netzwerks kompromittiert hat [BIGIP2021h].

F5 fordert Kunden dazu auf, die bereitgestellten Softwareupdates schnellstmöglich zu installieren. Mitunter werden jedoch noch nicht für alle Produkte bzw. Versionen Fixes angeboten. In diesen Fällen können Mitigationsmaßnahmen des Herstellers in Betracht gezogen werden, die ebenfalls unter [BIGIP2020b] bis [BIGIP2021h] zu finden sind. Außerdem stellt das Unternehmen Vorfallsindikatoren und Handlungsempfehlungen zum Verhalten im Angriffsfall zur Verfügung [BIGIP2021i]. Häufige Fragen beantwortet F5 unter [BIGIP2021a].

## Bewertung

**Vier der identifizierten Schwachstellen werden mit CVSS-Scores von >9 als „kritisch“ eingestuft.** Insbesondere von CVE-2021-22986 geht - bei Erreichbarkeit der BIG-IP Management Schnittstelle - ein grundsätzliches, konfigurationsunabhängiges Risiko für Netzwerke von Organisationen aus. Die **Veröffentlichung verschiedener PoC-Skripte und die Beobachtung von Angriffen** auf BIG-IP/BIG-IQ Systeme unterstreichen die Dringlichkeit zur Umsetzung der empfohlenen Schutzmaßnahmen.

## Maßnahmen

**Das BSI empfiehlt das kurzfristige Einspielen der von F5 bereitgestellten Patches** – auch dann, wenn die zur Ausnutzung notwendigen, genannten Bedingungen nicht vorliegen. Sollte verwundbare Software eingesetzt werden, für die noch keine Updates zur Verfügung stehen, sind die vom Hersteller aufgeführten Mitigationsmaßnahmen zu beachten.

Besteht Grund zur Annahme, dass bereits ein Angriff stattgefunden hat, sollten außerdem die unter [BIGIP2021i] empfohlenen Maßnahmen in Betracht gezogen werden. Indikatoren zur Detektion sind sowohl dort als auch unter [NCC2021] zu finden.

## Links

[CER2021] CB-K21/0261 F5 BIG-IP: Mehrere Schwachstellen  
<https://cert-bund.de/advisoryshort/CB-K21-0261%20UPDATE%204>

[BIGIP2021a] F5 - K02566623: Overview of F5 critical vulnerabilities  
<https://support.f5.com/csp/article/K02566623>

[BIGIP2021b] F5 - K03009991: iControl REST unauthenticated remote command execution vulnerability CVE-2021-22986  
<https://support.f5.com/csp/article/K03009991>

[BIGIP2021c] F5 - K18132488: Appliance mode TMUI authenticated remote command execution vulnerability CVE-2021-22987  
<https://support.f5.com/csp/article/K18132488>

[BIGIP2021d] F5 - K70031188: TMUI authenticated remote command execution vulnerability CVE-2021-22988  
<https://support.f5.com/csp/article/K70031188>

[BIGIP2021e] F5 - K56142644: Appliance mode Advanced WAF/ASM TMUI authenticated remote command execution vulnerability CVE-2021-22989

<https://support.f5.com/csp/article/K56142644>

[BIGIP2021f] F5 - K45056101: Advanced WAF/ASM TMUI authenticated remote command execution vulnerability CVE-2021-22990

<https://support.f5.com/csp/article/K45056101>

[BIGIP2021g] F5 - K56715231: TMM buffer-overflow vulnerability CVE-2021-22991

<https://support.f5.com/csp/article/K56715231>

[BIGIP2021h] F5 - K52510511: Advanced WAF/ASM buffer-overflow vulnerability CVE-2021-22992

<https://support.f5.com/csp/article/K52510511>

[BIGIP2021i] F5 - K11438344: Considerations and guidance when you suspect a security compromise on a BIG-IP system

<https://support.f5.com/csp/article/K11438344>

[NCC2021] NCC Group - RIFT: Detection capabilities for recent F5 BIG-IP/BIG-IQ iControl REST API vulnerabilities CVE-2021-22986

<https://research.nccgroup.com/2021/03/18/rift-detection-capabilities-for-recent-f5-big-ip-big-iq-icontrol-rest-api-vulnerabilities-cve-2021-22986/>

[TWI2021] Twitter-Post: Security updates for #F5#BIG-IP and #BIG-IQ systems #PATCHNOW

<https://twitter.com/certbund/status/1369984106453434370>

# 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.