



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

# F5-Produkte durch verschiedene Schwachstellen verwundbar

CSW-Nr. 2021-243177-1032, Version 1.0, 26.08.2021

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

Am 24. August 2021 informierte der Netzerkäufer F5 auf seiner Homepage über insgesamt 29 Schwachstellen in seinen Produkten [F5AD]. 13 der veröffentlichten Sicherheitslücken werden entsprechend Common Vulnerability Scoring System (CVSS) mit einem Schweregrad von „hoch“ bewertet. Von besonderer Bedeutung ist hier die Schwachstelle mit der Nummer CVE-2021-23031, bei der ein Angreifer eine Privilegien-Eskalation herbeiführen kann [F5AD]. Ist bei den betroffenen Produkten BIG-IP Advanced WAF (Web Application Firewall) und Application Security Manager (ASM) sowie Traffic Management User Interface (TMUI) der Appliance Mode aktiviert, muss die CVSS-Bewertung sogar auf „kritisch“ heraufgestuft werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hatte auf diesen Sachverhalt zeitnah über seinen Warn- und Informationsdienst [CER2021] hingewiesen.

Folgende Produkte und Serien aus dem F5-Portfolio sind von den schwerwiegenden Sicherheitslücken betroffen:

- BIG IP,
- BIG IQ,
- Advanced WAF,
- iControl sowie
- TMUI und

\* 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.

- Traffic Management Microkernel (TMM).

Weiterhin wurden auch für andere Produkte Schwachstellen bekannt. Diese werden nach CVSS mit „mittel“ oder „gering“ bewertet. Für viele der genannten Schwachstellen hat F5 bereits Patches zur Verfügung gestellt. In ausgewählten Fällen kann außerdem ein Hotfix beim Hersteller angefordert werden. Für die ebenfalls betroffene Lösung BIG IQ, mit der BIG IP-Produkte zentral verwaltet werden können, ist noch kein Update verfügbar.

Produkte von F5 sind in zahlreichen Organisationen verschiedenster Branchen zu finden.

## Bewertung

Aufgrund ihrer zentralen Bedeutung in IT-Umgebungen sind Netzwerkkomponenten – wie im vorliegenden Fall – grundsätzlich ein attraktives Ziel für Cyber-Angriffe. Es muss daher davon ausgegangen werden, dass sich Täter die veröffentlichten Schwachstellen kurzfristig zu Nutze machen werden.

## Maßnahmen

Das BSI empfiehlt das kurzfristige Einspielen der von F5 bereitgestellten Patches [F5AD]. Sofern dies aus unterschiedlichen Gründen nicht möglich ist, sind die auf den Detailseiten zu den jeweiligen Schwachstellen aufgeführten Mitigationsmaßnahmen zu beachten.

Beim Patchen sollten die Empfehlungen gemäß BSI-Grundschutz beachtet werden [BSI2021a]. Allgemeine Hinweise zur Absicherung und dem Aufbau von Firewalls stellt das BSI im Grundschutz-Kompendium bereit [BSI2021b].

## Links

[F5AD] - K50974556: Overview of F5 vulnerabilities (August 2021)

<https://support.f5.com/csp/article/K50974556>

[CER2021] - CB-K21/0261 F5 BIG-IP: Mehrere Schwachstellen

<https://www.cert-bund.de/advisoryshort/CB-K21-0903>

[BSI2021a] Patch - und Änderungsmanagement

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium\\_Einzel\\_PDFs/04\\_OPS\\_Betrieb/OPS\\_1\\_1\\_3\\_Patch\\_und\\_Aenderungsmanagement\\_Edition\\_2020.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/04_OPS_Betrieb/OPS_1_1_3_Patch_und_Aenderungsmanagement_Edition_2020.pdf)

[BSI2021b] - NET.3.2: Firewall (Edition 2021)

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium\\_Einzel\\_PDFs\\_2021/09\\_NET\\_Netze\\_und\\_Kommunikation/NET\\_3\\_2\\_Firewall\\_Edition\\_2021.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/09_NET_Netze_und_Kommunikation/NET_3_2_Firewall_Edition_2021.pdf)

# 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.