

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200330.3 | 30 марта 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в продуктах компании F5 BIG-IP и BIG-IQ

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator) BIG-IQ Centralized Management
Дата выявления	27 марта 2017 г.
Дата обновления	30 марта 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-5858	<p>Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольные команды с повышенными привилегиями в целевой системе посредством использования специально созданной команды «tmsh». Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSS:3.0: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-77: Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)</p>	7,8

	<p>Рекомендации по устранению: обновить программное обеспечение или воспользоваться инструкцией, указанной по ссылке ниже. https://support.f5.com/csp/article/K36814487</p>	
<p>MITRE: CVE-2020-5857</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена некорректной обработкой HTTP-запросов.</p> <p>CVSS:3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных</p> <p>Рекомендации по устранению: обновить программное обеспечение или воспользоваться инструкцией, указанной по ссылке ниже. https://support.f5.com/csp/article/K70275209</p>	7,5
<p>MITRE: CVE-2020- 5859</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально созданных сообщений по протоколу HTTP/3. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSS:3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных</p> <p>Рекомендации по устранению: обновить программное обеспечение или воспользоваться инструкцией, указанной по ссылке ниже. https://support.f5.com/csp/article/K61367237</p>	7,5

Ссылки на
источники

<https://www.cybersecurity-help.cz/vdb/SB2020033010>