安全漏洞通告

【更新:POC 公开】F5 多个严重漏洞通告

360CERT
北京奇虎科技有限公司 | 2021-03-11

报告信息

报告名称	【更新:POC 公开】F5 多个严重漏洞通告		
报告类型	安全漏洞通告	**报告编号**	B6-2021-031901
报告版本	1	**报告日期**	2021-03-11
报告作者	360CERT	**联系方式**	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-03-11	360CERT	360CERT	撰写报告

目录

一、 漏洞档案

漏洞类型	溢出
CVE 编号	CVE-2021-22992 等
相关厂商	F5
相关组件	暂无
威胁等级	严重
影响面	广泛
360CERT 评分	9.8
修复方案	通用修补方案/临时修补方案
漏洞发布时间	2021-03-11
报告生成时间	2021-03-11

二、 漏洞简述

2021 年 03 月 19 日，360CERT 监测发现 CVE-2021-22986 的 POC 已经公开。本次更新漏洞状态及复现截图。具体更新详情可参考漏洞详情。

2021 年 03 月 11 日，360CERT 监测发现 F5 发布了 F5 BIG-IQ/F5 BIG-IP 代码执行,代码执行 的风险通告，该漏洞编号为 CVE-2021-22986,CVE-2021-22987,CVE-2021-22992.CVE-2021-22991 ，漏洞等级：严重，漏洞评分：9.8。

三、 漏洞评级

经过安全技术人员的分析，最终对该漏洞的评定结果如下

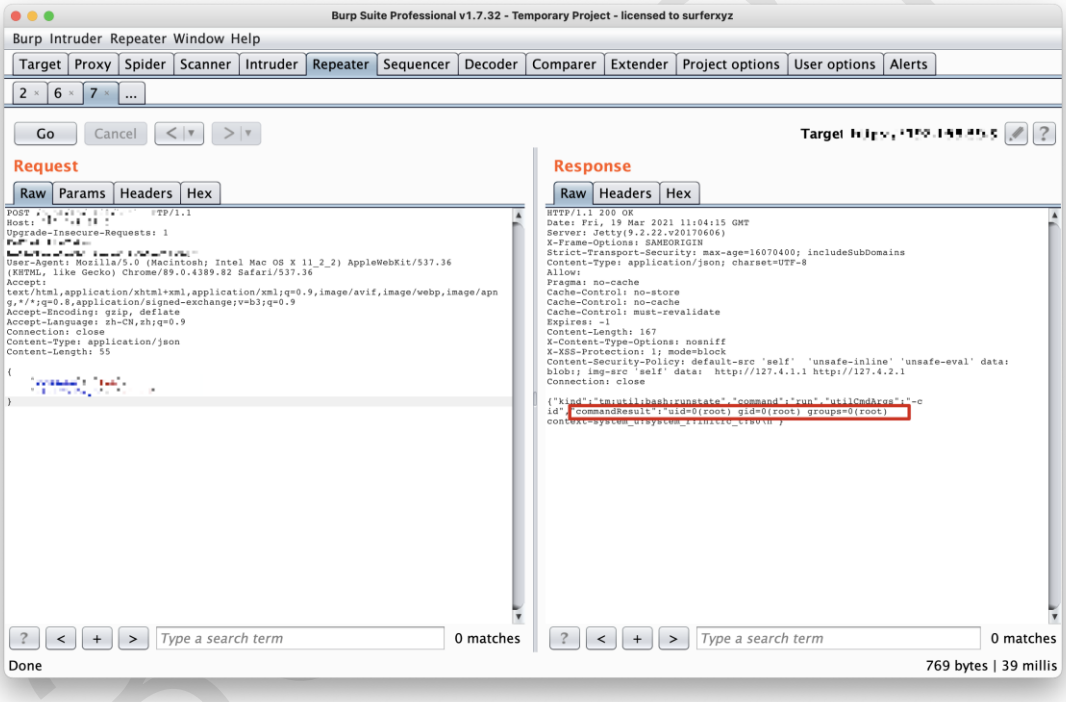
评定方式	等级
威胁等级	严重
影响面	广泛
360CERT 评分	9.8

四、 漏洞详情

CVE-2021-22986: 代码执行漏洞

该漏洞允许未经身份验证的攻击者通过 BIG-IP 管理界面和自身 IP 地址对 iControl REST 接口进行网络访问，以执行任意系统命令，创建或删除文件以及禁用服务。 该漏洞只能通过控制界面利用，而不能通过数据界面利用。

目前 360CERT 利用公开的 poc，已经成功复现该漏洞，复现截图如下：



CVE-2021-22987: 代码执行漏洞

当以设备模式运行时，该漏洞允许经过身份验证的用户通过 BIG-IP 管理端口或自身 IP 地址对配置实用程序进行网络访问，以执行任意系统命令，创建或删除文件或禁用服务。 该漏洞只能通过控制界面利用，而不能通过数据界面利用。漏洞利用可能导致系统完全受损并破坏设备模式。

CVE-2021-22991：缓冲区溢出漏洞

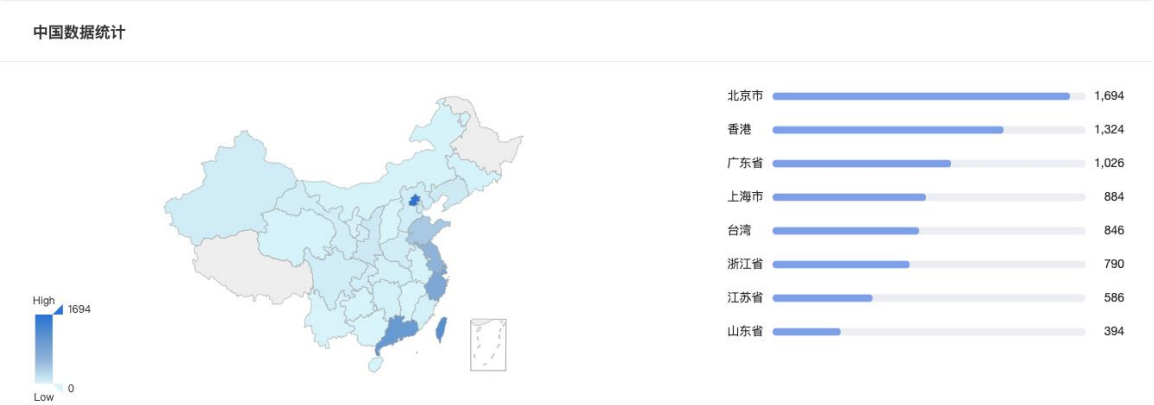
流量管理微内核(Traffic Management Microkernel, TMM) URI 的规范化可能会错误地处理对虚拟服务器的请求，从而触发缓冲区溢出，导致 DoS 攻击。在某些情况下，它可能绕过基于 URL 的访问控制或造成远程代码执行。该漏洞只能通过控制界面利用，而不能通过数据界面利用。

CVE-2021-22992：缓冲区溢出漏洞

对在登录页面的策略中配置了 Advanced WAF / ASM 虚拟服务器的恶意 HTTP 响应可能会触发缓冲区溢出，从而导致 DoS 攻击。在某些情况下，可能造成远程代码执行。该漏洞只能通过控制界面利用，而不能通过数据界面利用。

五、 相关空间测绘数据

360 安全大脑-Quake 网络空间测绘系统通过对全网资产测绘，发现 f5 具体分布如下图所示。



六、 影响版本

CVE-2021-22986

BIG-IP：

- 16.0.0-16.0.1

- 15.1.0-15.1.2

-14.1.0-14.1.3.1

- 13.1.0-13.1.3.5

- 12.1.0-12.1.5.2

BIG-IQ：

- 7.1.0-7.1.0.2

- 7.0.0-7.0.0.1

- 6.0.0-6.1.0

CVE-2021-22987/CVE-2021-22992

BIG-IP：

- 16.0.0-16.0.1

- 15.1.0-15.1.2

- 14.1.0-14.1.3.1

- 13.1.0-13.1.3.5

- 12.1.0-12.1.5.2

- 11.6.1-11.6.5.2

CVE-2021-22991

BIG-IP：

- 16.0.0-16.0.1
- 15.1.0-15.1.2
- 14.1.0-14.1.3.1
- 13.1.0-13.1.3.5
- 12.1.0-12.1.5.2

七、 漏洞列表

编号	描述	导致结果	威胁等级
CVE-2021-22992	溢出	任意代码执行	严重
CVE-2021-22991	溢出	任意代码执行	严重
CVE-2021-22986	代码执行	任意代码执行	严重
CVE-2021-22987	代码执行	任意代码执行	严重

八、 安全建议

(一) 通用修补方案

CVE-2021-22987:

BIG-IP 16.0.0 - 16.0.1 版本升级到 16.0.1.1

BIG-IP 15.1.0 - 15.1.2 版本升级到 15.1.2.1

BIG-IP 14.1.0 - 14.1.3 版本升级到 14.1.4

BIG-IP 13.1.0 - 13.1.3 版本升级到 13.1.3.6

BIG-IP 12.1.0 - 12.1.5 版本升级到 12.1.5.3

BIG-IP 11.6.1 - 11.6.5 版本升级到 11.6.5.3

CVE-2021-22986:

BIG-IP 16.0.0 - 16.0.1 版本升级到 16.0.1.1

BIG-IP 15.1.0 - 15.1.2 版本升级到 15.1.2.1

BIG-IP 14.1.0 - 14.1.3 版本升级到 14.1.4

BIG-IP 13.1.0 - 13.1.3 版本升级到 13.1.3.6

BIG-IP 12.1.0 - 12.1.5 版本升级到 12.1.5.3

BIG-IQ 7.1.0/7.0.0 对应升级到 7.1.0.3/7.0.0.2，或者升级到 8.0 版本

CVE-2021-22991:

BIG-IP16.0.0 - 16.0.1 版本升级到 16.0.1.1

BIG-IP15.1.0 - 15.1.2 版本升级到 15.1.2.1

BIG-IP14.1.0 - 14.1.3 版本升级到 14.1.4

BIG-IP13.1.0 - 13.1.3 版本升级到 13.1.3.6

BIG-IP12.1.0 - 12.1.5 版本升级到 12.1.5.3

(二) 临时修补方案

CVE-2021-22986

通过自身 IP 地址禁止访问 iControl REST：将系统中每个自身 IP 地址的 Port Lockdown 选项设置更改为 Allow None。 如果必须开放某端口，则开启 Allow Custom 选项。 默认情况下，iControl REST 监听 443 端口。

通过管理接口禁止访问 iControl REST：将管理访问权限限制为受信任用户和设备。

CVE-2021-22987

通过自身 IP 地址阻止访问 BIG-IP 系统配置实用程序：将系统上每个自身 IP 地址的 Port Lockdown 选项设置更改为 Allow None。 如果必须开放某端口，则开启 Allow Custom 选项。默认情况下，配置实用程序监听 443 端口。

通过管理接口禁止访问配置实用程序：将管理访问权限限制为受信任用户和 F5 设备。

CVE-2021-22992

- 使用 iRule 缓解恶意连接：

1. 登录配置实用程序

2. 找到 Local Traffic > iRules > iRule List

3. 选择 Create

4. 输入 iRule 的名称

5. 为了定义，添加以下 iRule 代码:

```
# Mitigation for K52510511: Advanced WAF/ASM Buffer Overflow
vulnerability CVE-2021-22992
when RULE_INIT {
# Set static::debug 1 to enable debug logging.
    set static::debug 0
    set static::max_length 4000
}
when HTTP_REQUEST {
    if {$static::debug}{
        set LogString "Client [IP::client_addr]:[TCP::client_port] ->
[HTTP::host][HTTP::uri]"
}
        set uri [string tolower [HTTP::uri]]
}
when HTTP_RESPONSE {
    set header_names [HTTP::header names]
    set combined_header_name [join $header_names ""]
    set combined_header_name_len [string length
$combined_header_name]
    if {$static::debug}{
        log local0. "================response====================="
        log local0. "$LogString (response)"
        log local0. "combined header names: $combined_header_name"
        foreach aHeader [HTTP::header names] {
        log local0. "$aHeader: [HTTP::header value $aHeader]"
}
        log local0. "the length of the combined response header
names: $combined_header_name_len"
        log local0. "============================================="
}
    if { ( $combined_header_name_len > $static::max_length ) } {
```

```
        log local0. "In the response of '$uri', the length of the
combined header names $combined_header_name_len exceeds the maximum
value $static::max_length. See K52510511: Advanced WAF/ASM Buffer
Overflow vulnerability CVE-2021-22992"
HTTP::respond 502 content "<HTML><HEAD><TITLE>Bad
Gateway</TITLE></HEAD> <BODY><P>The server response is invalid.
Please inform the administrator. Error: K52510511</P></BODY></HTML>"
}
}
```

6. 选择 Finished

7. 将 iRule 与受影响的虚拟服务器相关联

- 修改登录界面配置：

1. 登录到受影响的 BIG-IP Advanced WAF / ASM 系统的配置实用程序

2. 找到 Security > Application Security > Sessions and Logins > Login Pages List

3. 从 Current edited policy lis 中选择安全策略

4. 从这两个设置中删除所有配置

5. 选择保存以保存更改

6. 选择 Apply Policy，应用更改

7. 选择 OK 确认操作

- 删除登陆界面：

1. 登录到受影响的 BIG-IP Advanced WAF / ASM 系统的配置实用程序。

2. 找到 Security > Application Security > Sessions and Logins > Login Pages List

3. 选择要删除的登录页面配置

4. 选择 Delete。

5. 选择 OK 确认删除

6. 选择 Apply Policy，应用更改

7. 选择 OK 确认操作

九、 产品侧解决方案

(一) 360 城市级网络安全监测服务

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台(quake.360.cn)，通过资产测绘技术的方式，对该漏洞进行监测。可联系相关产品区域负责人或(quake#360.cn)获取对应产品。

十、 参考链接

1. F5 官方通告

   https://support.f5.com/csp/article/K02566623

2. F5 从认证绕过到远程代码执行漏洞分析

   https://blog.riskivy.com/f5%e4%bb%8e%e8%ae%a4%e8%af%81%e7%bb%95%e8%bf%87%e5%88%b0%e8%bf%9c%e7%a8%8b%e4%bb%a3%e7%a0%81%e6%89%a7%e8%a1%8c%e6%bc%8f%e6%b4%9e%e5%88%86%e6%9e%90/

附录 A 报告风险等级说明

360CERT 评分是依托 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. 9.0 ≤ 360CERT 评分 ≤ 10 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 任意攻击者可直接发起攻击 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	1. 4.0 ≤ 360CERT 评分 < 7 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 a) 占用存储空间 b) 降低执行效率 4. 获得平台用户级权限
危害结果	1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	1. 0 ≤ 360CERT 评分 < 4 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

附录 B 影响面说明

影响面说明	
广泛	影响主体数 > 10w 底层依赖库
一般	5w < 影响主体数 < 10w 开源库
局限	影响主体数 < 5w 特制版本的

附录 C 360 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在"CVSS 漏洞评分体系"的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 – 10.0	严重
7.0 – 8.9	高危
4.0 – 6.9	中危
0 - 3.9	低危