BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 57 /TTCNTT-KTHT
V/v 07 lỗ hổng bảo mật trong thiết bị F5 BIG-IP

Hà Nội, ngày 17 tháng 3 năm 2021

Kính gửi: Các đơn vị có hệ thống công nghệ thông tin trực thuộc Bộ

Ngày 10/03/2021, F5 đã công bố 07 lỗ hổng bảo mật **(CVE-2021-22986, CVE-2021-22987, CVE-2021-22991, CVE-2021-22992, CVE-2021-22989, CVE-2021-22988, CVE-2021-22990)** trong các thiết bị, ảnh hưởng đến các phiên bản của sản phẩm F5 BIG-IP từ 11.X đến 16.X. Khai thác thành công các lỗ hổng này cho phép đối tượng tấn công chèn và thực thi mã tùy ý (thông tin chi tiết về các lỗ hổng có tại phụ lục kèm theo).

Theo thống kê tính đến tháng 3 năm 2021, có hơn 30.000 thiết bị trên Internet đang có nguy cơ bị tấn công bởi lỗ hổng bảo mật này. Qua đánh giá sơ bộ của Cục An toàn thông tin – Bộ Thông tin và Truyền thông, Việt Nam có hàng trăm hệ thống đang sử dụng sản phẩm F5 BIG-IP để bảo vệ các hệ thống thông tin, chống lại các tấn công an ninh mạng đa lớp hiện đang ảnh hưởng tới rất nhiều cơ quan tổ chức. Đây là những hệ thống đầu tiên nằm trong mục tiêu mà đối tượng tấn công sẽ tìm đến.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Trung tâm Công nghệ thông tin khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát, xác minh hệ thống thông tin có sử dụng thiết bị F5 và bị ảnh hưởng bởi lỗ hổng trên hay không để có phương án xử lý, khắc phục lỗ hổng. Quý đơn vị nên cập nhật, nâng cấp lên phiên bản mới nhất, trong trường hợp chưa kịp thời cập nhật được, nên có các biện pháp giảm thiểu thay thế để hạn chế nguy cơ bị tấn công (tham khảo tại phụ lục kèm theo).

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng. Đối với các cơ quan tổ chức có nhân sự kỹ thuật tốt có thể thử nghiệm xâm nhập vào hệ thống thông qua lỗ hổng này.

Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, điện thoại 024.39439060, thư điện tử: phongktht@most.gov.vn.

Trân trọng./

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Cổng thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

Phụ lục
Thông tin về các lỗ hổng bảo mật trong thiết bị F5 BIG-IP
(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021)

1. Thông tin các lỗ hổng bảo mật

TT	CVE	Mô tả	Link tham khảo hướng dẫn
1	CVE-2021-22986	Điểm CVSS: 9.8 (nghiêm trọng) Lỗi trong chức năng iControl REST, cho phép đối tượng tấn công thực thi mã từ xa.	https://support.f5.com/csp/article/K03009991
2	CVE-2021-22987	Điểm CVSS: 9.9 (nghiêm trọng) Lỗi trong giao diện TMUI, cho phép đối tượng tấn công với quyền người dùng (thấp) thực thi các lệnh tùy ý.	https://support.f5.com/csp/article/K18132488
3	CVE-2021-22991	Điểm CVSS: 9.0 (cao) Cho phép đối tượng tấn công gây ra lỗi tràn bộ đệm dẫn đến tấn công DoS, thực thi mã từ xa.	https://support.f5.com/csp/article/K56715231
4	CVE-2021-22992	Điểm CVSS: 9.0 (cao) Cho phép đối tượng tấn công gây ra lỗi tràn bộ đệm dẫn đến tấn công DoS, thực thi mã từ xa.	https://support.f5.com/csp/article/K52510511
5	CVE-2021-22988	Điểm CVSS: 8.8 (cao) Lỗi trong giao diện TMUI, cho phép đối tượng tấn công với quyền người dùng (cao) thực thi các lệnh tùy ý.	https://support.f5.com/csp/article/K70031188
6	CVE-2021-22989	Điểm CVSS: 8.0 (cao) Lỗi trong giao diện TMUI, cho phép đối tượng tấn công với quyền người dùng (cao)	https://support.f5.com/csp/article/K56142644

		thực thi các lệnh tùy ý.	
7	CVE-2021-22990	Điểm CVSS: 6.6 (trung bình) Lỗi trong giao diện TMUI, cho phép đối tượng tấn công với quyền người dùng (cao) thực thi các lệnh tùy ý.	https://support.f5.com/csp/article/K45056101

2. Thông tin các phiên bản ảnh hưởng và bản vá

CVE	Sản phẩm	Phiên bản ảnh hưởng	Phiên bản đã cập nhật bản vá
CVE-2021-22986	BIG-IP (LTM, AAM, Advanced WAF, AFM, Analytics, APM, ASM, DDHD, DNS, FPS, GTM, Link Controller, PEM, SSLO)	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	16.0.1.1 15.1.2.1 14.1.4 13.1.3.6 12.1.5.3
CVE-2021-22987	BIG-IP (LTM, AAM, Advanced WAF, AFM, Analytics, APM, ASM, DDHD, DNS, FPS, GTM, Link Controller, PEM, SSLO)	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	16.0.1.1 15.1.2.1 14.1.4 13.1.3.6 12.1.5.3 11.6.5.3
CVE-2021-22991	BIG-IP (LTM, AAM, Advanced WAF, AFM, Analytics, APM, ASM, DDHD, DNS, FPS, GTM, Link Controller, PEM, SSLO)	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	16.0.1.1 15.1.2.1 14.1.4 13.1.3.6 12.1.5.3
CVE-2021-22992	BIG-IP (Advanced WAF and ASM)	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	16.0.1.1 15.1.2.1 14.1.4 13.1.3.6 12.1.5.3

CVE-2021-22988	BIG-IP (LTM, AAM, Advanced WAF, AFM, Analytics, APM, ASM, DDHD, DNS, FPS, GTM, Link Controller, PEM, SSLO)	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	16.0.1.1 15.1.2.1 14.1.4 13.1.3.6 12.1.5.3 11.6.5.3
CVE-2021-22989	BIG-IP (Advanced WAF and ASM)	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	16.0.1.1 15.1.2.1 14.1.4 13.1.3.6 12.1.5.3 11.6.5.3
CVE-2021-22990	BIG-IP (Advanced WAF and ASM)	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	16.0.1.1 15.1.2.1 14.1.4 13.1.3.6 12.1.5.3 11.6.5.3

3. Hướng dẫn khắc phục

Phương án tốt nhất để khắc phục lỗ hổng bảo mật là thực hiện cập nhật các bản vá do hãng F5 phát hành. Trung tâm Công nghệ thông tin khuyến nghị Quý đơn vị nên cập nhật sớm nhất có thể.

Trong trường hợp chưa thể cập nhật ngay, các quản trị viên nên thực hiện các bước thay thế tạm thời để giảm thiểu nguy cơ tấn công (trừ lỗ hổng CVE-2021-22991 chưa có biện pháp giảm thiểu tạm thời):

3.1. Đối với 05 lỗ hổng (CVE-2021-22986, CVE-2021-22987, CVE-2021-22988, CVE-2021-22989, CVE-2021-22990):

1. Chặn quyền truy cập tới chức năng iControl REST và Configuration utility thông qua địa chỉ IP

- Thay đổi cài đặt **Port Lockdown** về **Allow None** cho mỗi địa chỉ IP trong hệ thống.
- Nếu cần thiết phải mở một số ports thì cần sử dụng tính năng Allow Custom, chú ý không mở port của chức năng iControl REST và Configuration utility mặc định ở port 443.

2. Chặn quyền truy cập iControl REST và Configuration utiửty thông qua giao diện quản lý

Để giảm thiểu lỗ hổng này cho các sản phẩm F5 bị ảnh hưởng, các quản trị viên chỉ nên hạn chế quyền truy cập quản lý đối với những người dùng và thiết bị đáng tin cậy qua mạng an toàn (như quản lý mật khẩu và tài khoản người dùng, quản lý truy cập mạng, quản lý quyền truy cập cổng quản trị, quản lý các dịch vụ và các mô-đun bổ sung,...) Để biết thêm thông tin về cách đảm bảo quyền truy cập vào hệ thống BIG-IP, tham khảo các bài viết sau:

- https://support.f5.com/csp/article/K13092

- https://support.f5.com/csp/article/K46122561

- https://support.f5.com/csp/article/K69354049

3.2. Đối với CVE-2021-22991: hiện tại tạm thời chưa có biện pháp giảm thiểu thay thế, vì vậy Trung tâm Công nghệ thông tin, khuyến nghị Quý đơn vị cần cập nhật bản vá sớm nhất có thể.

3.3. Đối với CVE-2021-22992:

1. Hạn chế các kết nối độc hại bằng iRule

- Đăng nhập vào Configuration utility

- Chọn **Local Trafic/iRules/iRule List**

- Chọn **Create**

- Đặt tên cho iRule

- Trong **Definition,** add thêm lệnh iRule:

```
# Mitigation for K52510511: Advanced WAF/ASM Buffer Overtlow 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 $combined_header_name]
    if {Sstatic:: debug} {
        log local0. "==================response================="
        log local0. "$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>"
}
}
```

- Chọn **Finished**

- Liên kết iRule với các máy chủ ảo bị ảnh hưởng

2. Sửa đổi cấu hình trong giao diện đăng nhập

- Đăng nhập vào Configuration utility của hệ thống BIG-IP WAF/ASM

- Chọn **Security** > **Application Security** > **Sessions and Logins** > **Login Pages List.**

- Chọn chính sách bảo mật

- Chọn tên của URL đăng nhập từ **Login Pages List.**

- Xóa tất cả cấu hình khỏi cả 2 cài đặt

- Chọn **Save** để lưu thay đổi

- Chọn **Apply Policy** để áp dụng các thay đổi.

- Chọn **OK** để xác nhận.

3. Harden pool members

Để giảm thiểu lỗ hổng này, bạn có thể tăng cường các máy chủ web và mạng back-end của mình để ngăn chặn các tiêu đề độc hại trong phản hồi HTTP tới trang đăng nhập được gửi đến hệ thống BIG-IP Advanced WAF/ASM.

4. Xóa các trang đăng nhập

- Đăng nhập vào Configuration utility của hệ thống BIG-IP ASM

- Chọn **Security > Application Security > Sessions and Logins > Login Pages List.**

- Chọn chính sách bảo mật

- Chọn cấu hình trang đăng nhập muốn xóa

- Chọn **Delete**

- Chọn **OK** để xác nhận xóa

- Chọn **Apply Policy** để áp dụng thay đổi

- Chọn **OK** để xác nhận.

Tham khảo chi tiết tại: https://support.f5.com/csp/article/K52510511

DANH SÁCH CÁC ĐƠN VỊ CÓ HỆ THỐNG CNTT

(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021)

STT	Tên đơn vị
1	Cục Thông tin khoa học và công nghệ quốc gia
2	Cục Sở hữu trí tuệ
3	Tổng cục Tiêu chuẩn Đo lường Chất lượng
4	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
5	Viện Năng lượng nguyên tử Việt Nam
6	Viện Khoa học sở hữu trí tuệ
7	Quỹ phát triển khoa học và công nghệ quốc gia
8	Cục An toàn bức xạ và hạt nhân
9	Quỹ đổi mới công nghệ quốc gia
10	Ban Quản lý Khu công nghệ cao Hòa Lạc