

Số: **515** /TB-SGDĐT

Quảng Ngãi, ngày **10** tháng 5 năm 2022

THÔNG BÁO

Cảnh báo lỗ hổng bảo mật CVE-2022-1388 ảnh hưởng nghiêm trọng trong sản phẩm BIG-IP

Theo đề nghị của Sở Thông tin và Truyền thông tại Công văn số 602/STTTT-BCVT&CNTT ngày 09/5/2022 về việc Cảnh báo lỗ hổng bảo mật CVE-2022-1388 ảnh hưởng nghiêm trọng trong sản phẩm BIG-IP;

Sở Giáo dục và Đào tạo thông báo đến các đơn vị, cơ sở giáo dục kiểm tra, rà soát để phát hiện và xử lý kịp thời các hệ thống thông tin có khả năng bị ảnh hưởng bởi lỗ hổng bảo mật CVE-2022-1388 trong sản phẩm BIG-IP. (Kèm theo Phụ lục Công văn số 602/STTTT-BCVT&CNTT ngày 09/5/2022 của Sở Thông tin và Truyền thông).

Khi phát hiện các hệ thống có biểu hiện bị khai thác, tấn công mạng, triển khai ngay các biện pháp xử lý ngăn chặn tấn công trên hệ thống và thông báo về Văn phòng Sở Giáo dục và Đào tạo để phối hợp Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi có các biện pháp hỗ trợ, xử lý kịp thời.

Yêu cầu lãnh đạo các đơn vị quan tâm chỉ đạo thực hiện./.

Nơi nhận:

- Đơn vị trực thuộc Sở GDĐT;
- Phòng GDĐT huyện, thị xã, thành phố;
- Trung tâm GDNN-GDTX huyện, thị xã;
- Lãnh đạo Sở GDĐT;
- Các phòng thuộc Sở GDĐT;
- Lưu: VT, VP, ndh.

TL. GIÁM ĐỐC
KT. CHÁNH VĂN PHÒNG
PHÓ CHÁNH VĂN PHÒNG



Nguyễn Đức Huân

PHỤ LỤC

THÔNG TIN VỀ LỖ HỒNG BẢO MẬT CVE-2022-1388

(Kèm theo Công văn số 602/STTTT-BCVT&CNTT ngày 09/5/2022 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hồng bảo mật

- **Mô tả:** Lỗ hồng tồn tại trong BIG-IP iControl REST cho phép đối tượng tấn công không cần xác thực có thể thực thi lệnh tùy ý, chiếm quyền điều khiển hệ thống.

- **Điểm CVSS:** 9.8 (Nghiêm trọng).

- **Ảnh hưởng:**

Sản phẩm	Phiên bản	Phiên bản bị ảnh hưởng	Bản vá
BIG-IP (all modules)	17.x	None	17.0.0
16.x	16.1.0 – 16.1.2	16.1.2.2	
15.x	15.1.0 – 15.1.5	15.1.5.1	
14.x	14.1.0 – 14.1.4	14.1.4.6	
13.x	13.1.0 – 13.1.4	13.1.5	
12.x	12.1.0 – 12.1.6	Không hỗ trợ	
11.x	11.6.1 – 11.6.5	Không hỗ trợ	

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hồng bảo mật nói trên theo hướng dẫn của hãng. Quý đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại mục 1 của phụ lục.

Trong trường hợp chưa thể cập nhật bản vá, Quý đơn vị cần thực hiện các bước khắc phục thay thế để giảm nguy cơ bị tấn công như sau:

2.1. Chặn quyền truy cập iControl REST thông qua địa chỉ IP

Thay đổi cài đặt **Port Lockdown** thành **Allow None** cho từng địa chỉ IP riêng trên hệ thống. Trong trường hợp cần phải mở bất kỳ cổng nào, quản trị viên nên sử dụng tùy chọn **Allow Custom** (chú ý để không cho phép truy cập vào iControl REST).

Lưu ý: Việc thực hiện hành động này sẽ ngăn chặn tất cả quyền truy cập vào Configuration utility và iControl REST thông qua địa chỉ IP riêng. Những thay đổi này cũng có thể ảnh hưởng đến các dịch vụ khác, bao gồm cả việc phá vỡ cấu hình High Availability (HA).

2.2. Chặn quyền truy cập iControl REST thông qua giao diện quản lý

Quản trị viên nên hạn chế quyền truy cập vào giao diện quản lý đối với những người dùng và thiết bị đáng tin cậy. Để biết thêm thông tin và cách đảm bảo quyền truy cập vào hệ thống thông tin BIG-IP, tham khảo tại:

- <https://support.f5.com/csp/article/K13092>
- <https://support.f5.com/csp/article/K46122561>
- <https://support.f5.com/csp/article/K69354049>

Lưu ý: Việc hạn chế quyền truy cập vào giao diện quản lý bằng địa chỉ IP trong **httpd** không phải là một biện pháp khắc phục khả thi.

2.3. Sửa đổi cấu hình BIG-IP httpd

Đối với các phiên bản BIG-IP 14.1.0 trở lên, BIG-IP 14.0.0 trở về trước, BIG-IP 14.1.0 trở lên:

Bước 1: Đăng nhập vào TMOS Shell (**tmsh**) của hệ thống BIG-IP bằng lệnh sau:

```
tmsh
```

Bước 2: Mở cấu hình **httpd** để chỉnh sửa bằng cách nhập lệnh sau:

```
edit /sys httpd all-properties
```

Bước 3: Xác định dòng lệnh bắt đầu với **include none** và thay thế **none** với đoạn sau:

```
"<If \"%{HTTP:connection} =~ /close/i \">
RequestHeader set connection close
</If>
<ElseIf \"%{HTTP:connection} =~ /keep-alive/i \">
RequestHeader set connection keep-alive
</ElseIf>
<Else>
RequestHeader set connection close
</Else>"
```

Bước 4: Sau khi cập nhật lệnh **include**, sử dụng phím ESC để thoát khỏi chế độ tương tác của trình soạn thảo, cuối cùng lưu các thay đổi bằng lệnh sau:

```
:wq
```

Bước 5: Tại Save changes (y/n/e), chọn y để lưu các thay đổi.

Bước 6: Lưu cấu hình BIG-IP bằng cách nhập lệnh:

```
save /sys config
```

Đối với phiên bản BIG-IP 14.0.0 trở về trước:

Bước 1: Đăng nhập vào TMOS Shell (**tmsh**) của hệ thống BIG-IP bằng lệnh sau:

```
tmsh
```

Bước 2: Mở cấu hình **httpd** để chỉnh sửa bằng cách nhập lệnh sau:



```
edit /sys httpd all-properties
```

Bước 3: Xác định dòng lệnh bắt đầu với include none và thay thế none với đoạn sau:

```
"RequestHeader set connection close"
```

Bước 4: Sau khi cập nhật lệnh include, sử dụng phím ESC để thoát khỏi chế độ tương tác của trình soạn thảo, cuối cùng lưu các thay đổi bằng lệnh sau:

```
:wq
```

Bước 5: Tại Save changes (y/n/e), chọn y để lưu các thay đổi.

Bước 6: Lưu cấu hình BIG-IP bằng cách nhập lệnh:

```
save /sys config
```

3. Tài liệu tham khảo

<https://support.f5.com/csp/article/K23605346>

