

Số: **1112** /STTTT-CNTT-VT
V/v lỗ hổng bảo mật CVE-2022-1388 ảnh
hưởng Nghiêm trọng trong
sản phẩm BIG-IP

Đồng Nai, ngày **16** tháng 5 năm 2022

Kính gửi:

- Các cơ quan đảng, nhà nước trên địa bàn tỉnh;
- Các tổ chức chính trị - xã hội thuộc địa bàn tỉnh ;
- Viettel Đồng Nai, VNPT Đồng Nai, Mobifone Đồng Nai;
- Trung tâm Công nghệ thông tin tỉnh Đồng Nai.

Sở Thông tin và Truyền thông nhận văn bản 637/CATTT-NCSC ngày 05/5/2022 của Cục An toàn thông tin về việc lỗ hổng bảo mật CVE-2022-1388 ảnh hưởng Nghiêm trọng trong sản phẩm BIG-IP;

Theo văn bản trên, ngày 04/5/2022, F5 đã công bố thông tin về lỗ hổng bảo mật **CVE-2022-1388** ảnh hưởng Nghiêm trọng trong BIG-IP iControl REST, cho phép đối tượng tấn công không cần xác thực có thể thực thi lệnh tùy ý, tạo hoặc xóa tệp tin, vô hiệu hóa các dịch vụ (thông tin chi tiết lỗ hổng bảo mật có tại phụ lục kèm theo).

Qua đánh giá sơ bộ của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, Việt Nam có hàng trăm hệ thống đang sử dụng sản phẩm F5 BIG-IP để bảo vệ cho các hệ thống quan trọng trên nền tảng web như dịch vụ công, các hệ thống tài chính, hệ thống quản trị dữ liệu,...Do đó hệ thống này sẽ là mục tiêu mà các đối tượng tấn công ưu tiên, từ đó thực hiện các cuộc tấn công nguy hiểm hơn.

Để tăng cường đảm bảo an toàn thông tin mạng trên địa bàn tỉnh, Sở Thông tin và Truyền thông đề nghị Quý đơn vị chủ động thực hiện các biện pháp sau:

1. Kiểm tra, rà soát hệ thống thông tin có khả năng bị ảnh hưởng bởi lỗ hổng trên và có phương án xử lý, khắc phục lỗ hổng. Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công (tham khảo thông tin tại phụ lục kèm theo); đồng thời rà soát lại toàn bộ hệ thống thông tin của Quý đơn vị, thường xuyên kiểm tra, đánh giá để chủ động phát hiện và xử lý kịp thời các lỗ hổng bảo mật.

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp

thời các nguy cơ tấn công mạng.

3. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ais@mic.gov.vn hoặc Sở Thông tin và Truyền thông, điện thoại 0251.3810.269, thư điện tử: attt@dongnai.gov.vn.

Trân trọng./.

Nơi nhận:

- Như trên;
- UBND tỉnh (b/c);
- Giám đốc và Phó Giám đốc Sở;
- Lưu: VT, CNTT, Thịnh.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Võ Hoàng Khai

Phụ lục

Thông tin về lỗ hổng bảo mật CVE-2022-1388

(Kèm theo văn bản số 1112/STTTT-CNTT-VT ngày 16/5/2022 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật

- **Mô tả:** Lỗ hổng 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 hổng 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:

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. 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.

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 nhập 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 nhập 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>