UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 718 /STTTT-TTGSĐH
Về việc cảnh báo lỗ hổng bảo mật cao, nghiêm trọng CVE-2022-1388 và trong các sản phẩm Microsoft công bố tháng 5/2022.

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

Tây Ninh, ngày 18 tháng 5 năm 2022

Kính gửi:
- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các cơ quan tham mưu, giúp việc Tỉnh ủy;
- Mặt trận Tổ quốc và các Đoàn thể chính trị - xã hội;
- Các Sở, ban, ngành tỉnh;
- Các huyện, thị, thành ủy;
- UBND các huyện, thị xã, thành phố.

Thực hiện theo Công văn số 647/CATTT-NCSC và Công văn số 637/CATTT-NCSC của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh bảo các lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng *(Chi tiết lỗ hổng trong phụ lục kèm theo).*

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin cho người dùng, đơn vị và toàn bộ hệ thống của tỉnh, Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương thực hiện gấp các công việc cụ thể như sau:

1. Kiểm tra, xác định các thiết bị máy tính, phần mềm liên quan có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời theo hướng dẫn tại phụ lục để tránh nguy cơ bị tấn công.

2. Tăng cường kiểm tra, giám sát hệ thống mạng của đơn vị, địa phương, khi có phát hiện hoạt động tấn công mạng, đề nghị liên hệ Sở Thông tin và Truyền thông để phối hợp xử lý kịp thời.

Thông tin liên quan đề nghị liên hệ Ông Vương Duy Thanh - Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0932624462.

Trân trọng./.

Nơi nhận:
- Như trên;
- GĐ Sở (b/c);
- P. CNTTBCVT;
- Lưu: VT, TTGSĐH.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TÂY NINH

Nguyễn Trung Hiếu

PHỤ LỤC
THÔNG TIN CÁC LỖ HỔNG NGHIÊM TRỌNG

I. Lỗ hổng bảo mật CVE-2022-1388

1. Mô tả

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.

- Điểm **CVSS: 9.8** (Nghiêm trọng).

2. Ảnh hưởng

Sản phẩm	Phiên bản	Phiên bản bị ảnh hưởng	Bản vá lỗi
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

3. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục lỗ hổng này là nâng cấp lên phiên bản mới nhất theo hướng dẫn của hãng.

Trong trường hợp không thể nâng cấp do chưa thể cập nhật bản vá, Quý đơn vị có thể áp dụng các bước khắc phục thay thế để giảm nguy cơ bị tấn công như sau:

a) 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).

b) 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.

c) 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>
<Elself\"%{HTTP;connection}=~/keep-alive/i">
RequestHeader set connection keep-alive
</Elself>
<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 nhận 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 nhận lệnh:

```
save /sys config
```

4. Tài liệu tham khảo: https://support.f5.com/csp/article/K2360534

II. Các lỗ hổng bảo mật trong các sản phẩm Microsoft công bố tháng 5/2022

Ngày 10/5/2022, Microsoft đã phát hành danh sách bản vá tháng 5 với 74 lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý các lỗ hổng bảo mật sau:

1. Các lỗ hổng bảo mật có mức ảnh hưởng Nghiêm trọng

STT	CVE	Mô tả	Tham khảo
1	**CVE-2022-26925**	- Điểm CVE: 9.8 (nghiêm trọng) - Lỗ hổng trong Windows LSA cho phép đối tượng tấn công không cần xác thực có thể thực hiện tấn công giả mạo	Security Update Guide -

		(spoofing). Trong thực tế, lỗ hổng này đang được sử dụng kết hợp với NTLM relay attack, từ đó giúp đối tượng tấn công nâng cao đặc quyền trong hệ thống mục tiêu Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2022/2019/2016/2012/2008	Loading - Microsoft
2	**CVE-2022-26923**	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Active Directory Domain Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019/2022.	MSRC Researcher Portal (microsoft.com)
3	**CVE-2022-26937**	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022.	CVE-2022-29972 - Security Update Guide - Microsoft - Insight Software: CVE-2022-29972 Magnitude Simba Amazon Redshift ODBC Driver
4	**CVE-2022-29972**	Lỗ hổng trong Magnitude Simba Amazon Redshift ODBC Driver cho phép đối tượng thực thi mã từ xa.	CVE-2022-29972 - Security Update Guide - Microsoft - Insight Software: CVE-2022-29972 Magnitude Simba Amazon Redshift ODBC Driver
5	**CVE-2022-21978**	- Điểm CVSS: 8.2 (Cao) - Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.	CVE-2022-22017 - Security Update Guide - Microsoft - Remote Desktop Client Remote

		- Ảnh hưởng: Windows Server 2013/2016/2019	Code Execution Vulnerability
6	**CVE-2022-22017**	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Remote Desktop Protocol Client cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 11, Windows Server 2022.	Security Update Guide - Loading - Microsoft
7	**CVE-2022-29110**	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office Web Apps Server 2013, Microsoft Excel 2013/2016.	https://msrc.microsoft.com/update-guide/vulnerability/CV E-2022-29110
8	**CVE-2022-29108**	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2016/2019, Microsoft SharePoint Foundation 2013	https://msrc.microsoft.com/update-guide/vulnerability/CV E-2022-29108

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, địa phương tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo tại mục 2.1 của Phụ lục

3. Tài liệu tham khảo

Zero Day Initiative — The May 2022 Security Update Review