BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

Số: 439 /CNTT-YTĐT
V/v lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2022

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

Hà Nội, ngày 27 *tháng* 06 *năm 2022*

Kính gửi:

- Vụ, Cục, Tổng cục, Văn phòng Bộ, Thanh tra Bộ;
- Các đơn vị trực thuộc Bộ Y tế;
- Các Sở Y tế.

Cục Công nghệ thông tin nhận được công văn 869/CATTT-NCSC ngày 16/06/2022 của Cục An toàn thông tin về việc lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2022.

Ngày 14/6/2022, Microsoft đã phát hành danh sách bản vá tháng 6 với 55 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:

Các lỗ hổng bảo mật có mức ảnh hưởng Nghiêm trọng:

- Lỗ hổng bảo mật **CVE-2022-30190** (hay còn gọi là Follina) trong Windows Microsoft Support Diagnotic Tool (MSDT) cho phép đối tượng tấn công thực thi mã tùy ý.

- Lỗ hổng bảo mật **CVE-2022-30136** trong Windows Network File System cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa.

Các lỗ hổng bảo mật có mức ảnh hưởng Cao:

- Lỗ hổng bảo mật **CVE-2022-30163** trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-30139** trong Windows Lightweight Directory Access Protocol (LDAP) cho phép đối tượng tấn công thực thi mã từ xa.

- 02 lỗ hổng bảo mật **CVE-2022-30157, CVE-2022-30158** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-30165** trong Windows Kerberos cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-30173** Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-30174** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Cục Công nghệ thông tin trân trọng đề nghị Quý đơn vị:

1. Kiểm tra, rà soát, xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công (tham khảo thông tin 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; 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.

Trong trường hợp cần thiết, Quý Đơn vị liên hệ Trung tâm Dữ liệu y tế, Cục Công nghệ thông tin, Bộ Y tế (ThS. Hoàng Đăng Trị, điện thoại: 0987772483; Email: trihd.cntt@moh.gov.vn) để được hỗ trợ.

Trân trọng./.

Nơi nhận:
- Như trên;
- Trung tâm Dữ liệu y tế (để thực hiện);
- Lưu: VT, CNTT.

CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
BỘ Y TẾ

Đỗ Trường Duy

BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

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

PHỤ LỤC
THÔNG TIN VỀ LỖ HỔNG LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM MICROSOFT
(Kèm theo Công văn số /CNTT-YTĐT ngày / /2022 của Cục Công nghệ thông tin)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-30190 (Follina)	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Microsoft Support Diagnotic Tool (MSDT) cho phép đối tượng tấn công thực thi mã tùy ý. - Ảnh hưởng: Windows 7/8.1/10, Windows Server 2008/2012/2016.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190 Văn bản số 786/CATTT-NCSC về việc lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool phát hành ngày 01/6/2022.
2	CVE-2022-30136	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ trong Windows Network File System cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows Server 2012/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30136

3	CVE-2022-30163	- Điểm CVSS: 8.5 (Cao) - Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2008/2012/2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30163
4	CVE-2022-30139	- Điểm CVSS:7.5 (cao) - Lỗ hổng trong Windows Lightweight Directory Access Protocol (LDAP) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows Server 2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30139
5	CVE-2022-30157 CVE-2022-30158	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: SharePoint Server 2019, SharePoint Enterprise Server 2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30157 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30158
6	CVE-2022-30165	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Windows Kerberos cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows 10/11, Windows Server 2016/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30165
7	CVE-2022-30173	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Excel 2013/2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30173

8	CVE-2022-30174	- Điểm CVSS: 7.4 (Cao) - Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft 365 Apps, Microsoft Office LTSC 2021.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30174

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 link nguồn tham khảo tại mục 1 của phụ lục.

3. Tài liệu tham khảo

https://msrc.microsoft.com/update-guide/releaseNote/2022-Jun

https://www.zerodayinitiative.com/blog/2022/6/14/the-june-2022- security-update-review

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.

1. 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 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
```

3. Tài liệu tham khảo

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

BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

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

THÔNG TIN LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số /CNTT-YTĐT ngày / /2022 của Cục Công nghệ thông tin)

1. Thông tin lỗ hổng bảo mật

- Mô tả: Lỗ hổng này ảnh hưởng đến FortiOS và FortiProxy, cho phép đối tượng tấn công không cần xác thực, có thể thực hiện tấn công directory traversal.
- Điểm CVSS: 7.3 (cao)
- Ảnh hưởng: FortiGate phiên bản 7.0.1 và 7.0.0, FortiProxy phiên bản 7.0.0.

2. Hướng dẫn khắc phục

- Fortinet đã phát hành bản vá cho lỗ hổng bảo mật này tại FortiGate phiên bản 7.0.1 trở lên, FortiProxy phiên bản 7.0.1 trở lên. Vì vậy để khắc phục và tránh nguy cơ tấn công, Quý đơn vị cần cập nhật bản vá trong thời gian sớm.

3. Nguồn tham khảo

- https://www.fortiguard.com/psirt/FG-IR-21-181