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

Số: 359/TTCNTT-KTHT
V/v lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong các sản phẩm của Fortinet và Microsoft

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

Hà Nội, ngày 17 tháng 10 năm 2022

Kính gửi: Đơn vị chuyên trách CNTT/ATTT của các đơn vị trực thuộc Bộ Khoa học và Công nghệ

Thực hiện công tác ứng cứu sự cố, an toàn thông tin mạng, Trung tâm Công nghệ thông tin (TTCNTT) cảnh báo lỗ hổng bảo mật ảnh hưởng nghiêm trọng đến các sản phẩm của Fortinet và Microsoft, như sau:

- Ngày 07/10/2022, Fortinet đã công bố thông tin về lỗ hổng bảo mật CVE-2022-40684, ảnh hưởng nghiêm trọng trong các sản phẩm FortiOS và FortiProxy của mình. Lỗ hổng này cho phép đối tượng tấn công chưa xác thực chiếm quyền truy cập vào giao diện quản trị từ xa. Tại Việt Nam, một số nhóm tấn công mạng đã sử dụng lỗ hổng này để tấn công vào hệ thống thông tin của nhiều cơ quan, tổ chức *(Thông tin chi tiết lỗ hổng bảo mật có tại Phụ lục I gửi kèm theo).*

- Ngày 11/10/2022, Microsoft đã phát hành danh sách bản vá tháng 10 với 85 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 có mức ảnh hưởng cao và nghiêm trọng sau:

+ Lỗ hổng bảo mật **CVE-2022-41033** trong Windows COM + Event System Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã được một số nhóm tấn công khai thác trong thực tế.

+ 02 lỗ hổng bảo mật **CVE-2022-37987, CVE-2022-37989** trong Windows Client Server Run-time Subsystem (CSRSS) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

+ Lỗ hổng bảo mật **CVE-2022-37968** trong Azure Arc-enabled Kubernetes cluster Connect cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

+ 03 lỗ hổng bảo mật **CVE-2022-38048, CVE-2022-41043, CVE-2022-38001** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa, thu thập thông tin, tấn công giả mạo (Spoofing). Trong đó lỗ hổng **CVE-2022-**

41043 đã được công bố rộng rãi trên Internet.

+ 03 lỗ hổng bảo mật **CVE-2022-41036, CVE-2022-41037, CVE-2022-41038** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

+ Lỗ hổng bảo mật **CVE-2022-41031** trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa.

+ Lỗ hổng bảo mật **CVE-2022-37976** trong Active Directory Certificate Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

Thông tin chi tiết các lỗ hổng bảo mật có tại Phụ lục II kèm theo.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị đồng thời góp phần bảo đảm an toàn cho các hệ thống thông tin của Bộ Khoa học và Công nghệ, TTCNTT khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát các sản phẩm FortiOS, FortiProxy và Microsoft đang sử dụng có khả năng bị ảnh hưởng bởi lỗ hổng trên. 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 chủ động phát hiện kịp thời các nguy cơ tấn công mạng.

Trong trường hợp cần thiết, Quý đơn vị 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);
- Lưu: VT, KTHT.

GIÁM ĐỐC

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

Hà Quốc Trung

Phụ lục I

Thông tin về lỗ hổng bảo mật trong sản phẩm Fortinet

(Kèm theo Công văn số 359 /TTCNTT-KTHT ngày 17 /10/2022 của Trung tâm Công nghệ thông tin)

1. Thông tin các lỗ hổng bảo mật

- **Mô tả:** Lỗ hổng ảnh hưởng đến FortiOS và FortiProxy, cho phép đối tượng tấn công chưa xác thực có quyền truy cập vào giao diện quản trị từ xa thông qua HTTP/HTTPS requests độc hại.

- **Ảnh hưởng:** FortiOS phiên bản 7.0.0 đến 7.0.6; 7.2.0 đến 7.2.1, FortiProxy phiên bản 7.0.0 đến 7.0.6, 7.2.0.

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục lỗ hổng bảo mật nói trên là cập nhật lên phiên bản mới (FortiOS 7.0.7 và 7.2.2, FortiProxy 7.0.7 và 7.2.1). Trong trường hợp chưa thể nâng cấp, Quý đơn vị cần thực hiện biện pháp khắc phục tạm thời bằng cách thiết lập chính sách và hạn chế quyền truy cập các địa chỉ IP vào giao diện quản trị, triển khai xác thực đa yếu tố (MFA) để không bị lộ thông tin giao diện quản trị và tránh nguy cơ bị tấn công khai thác.

3. Tài liệu tham khảo

https://www.tenable.com/blog/cve-2022-40684-critical-authentication-bypass-in-fortios-and-fortiproxy

https://docs.fortinet.com/document/fortigate/7.2.2/fortios-release-notes/289806/resolved-issues

https://docs.fortinet.com/document/fortigate/7.2.0/best-practices/127480/user-authentication-for-management-network-access

Phụ lục II

Thông tin về lỗ hổng bảo mật trong sản phẩm Microsoft

(Kèm theo Công văn số 359 /TTCNTT-KTHT ngày17 /10/2022 của Trung tâm Công nghệ thông tin)

1. Thông tin các lỗ hổng bảo mật

Stt	CVE	Mô tả	Link tham khảo
1	CVE-2022-41033	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows COM + Event System Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã được một số nhóm tấn công khai thác trong thực tế. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41033
2	CVE-2022-37987 CVE-2022-37989	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong trong Windows Client Server Run-time Subsystem (CSRSS) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37987 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37989
3	CVE-2022-37968	- Điểm CVSS: 10 (Nghiêm trọng) - Lỗ hổng trong Azure Arc-enabled Kubernetes cluster Connect cho phép đối tượng tấn công thực hiện nâng cao	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37968

Stt	CVE	Mô tả	Link tham khảo
		đặc quyền. - Ảnh hưởng: Azure Stack Edge, Azure Arc-enabled Kubernetes cluster 1.6.19/1.5.8/1.7.18/1.8.11	
4	CVE-2022-38048 CVE-2022-41043 CVE-2022-38001	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa, thu thập thông tin, tấn công giả mạo (Spoofing). - Ảnh hưởng: Microsoft Office 2013/2016/2019, Office 365 Apps, Office LTSC.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38048 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41043 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38001
5	CVE-2022-41036 CVE-2022-41037 CVE-2022-41038	Điểm CVSS: 8.8 (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, SharePoint Foundation/Enterprise Server 2013.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41036 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41037 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41038

Stt	CVE	Mô tả	Link tham khảo
6	CVE-2022-41031	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft 365 Apps, Microsoft Office 2019/LTSC.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41031
7	CVE-2022-37976	Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Active Directory Certificate Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/ 2022	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37976

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-Oct

https://www.zerodayinitiative.com/blog/2022/10/11/the-october-2022-security-update-review

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số 359/TTCNTT-KTHT ngày17 /10/2022 của Trung tâm Công nghệ thông tin)

TT	Tên đơn vị
1.	Thanh tra Bộ
2.	Cục Công tác phía Nam
3.	Cục Ứng dụng và phát triển công nghệ
4.	Cục Năng lượng nguyên tử
5.	Cục Thông tin Khoa học và Công nghệ Quốc gia
6.	Cục Phát triển thị trường và doanh nghiệp khoa học và công nghệ
7.	Cục An toàn bức xạ và hạt nhân
8.	Cục Sở hữu trí tuệ
9.	Tổng cục Tiêu chuẩn Đo lường Chất lượng
10.	Ban quản lý khu công nghệ cao Hoà Lạc
11.	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
12.	Viện Khoa học và công nghệ Việt Nam - Hàn Quốc (VKIST)
13.	Viện Nghiên cứu sáng chế và Khai thác công nghệ
14.	Viện Năng lượng nguyên tử Việt Nam
15.	Viện Ứng dụng công nghệ
16.	Viện Đánh giá khoa học và Định giá công nghệ
17.	Viện Khoa học sở hữu trí tuệ
18.	Viện Nghiên cứu và Phát triển Vùng
19.	Văn phòng các Chương trình trọng điểm cấp nhà nước
20.	Văn phòng Công nhận chất lượng
21.	Văn phòng Đăng ký hoạt động khoa học và công nghệ
22.	Văn phòng các Chương trình khoa học và công nghệ quốc gia
23.	Báo Khoa học và Phát triển
24.	Tạp chí Khoa học và Công nghệ Việt Nam
25.	Nhà xuất bản Khoa học và Kỹ thuật
26.	Quỹ Phát triển khoa học và công nghệ quốc gia
27.	Quỹ Đổi mới công nghệ quốc gia
28.	Trung tâm Nghiên cứu và Phát triển truyền thông khoa học và công nghệ
29.	Trung tâm Nghiên cứu và Phát triển hội nhập khoa học và công nghệ quốc tế