UBND TỈNH ĐIỆN BIÊN
**SỞ GIÁO DỤC VÀ ĐÀO TẠO**

Số /SGDĐT-QLCL
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft tháng 10/2022

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

*Điện Biên, ngày tháng 10 năm 2022*

Kính gửi:
- Các phòng CMNV Sở Giáo dục và Đào tạo;
- Phòng Giáo dục và Đào tạo các huyện, thị xã, thành phố;
- Các đơn vị trực thuộc Sở Giáo dục và Đào tạo;
- Các trung tâm GDNN-GDTX cấp huyện.

Căn cứ Văn bản số 1547/CATTT-NCSC ngày 10/10/2022 của Cục An toàn thông tin về lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong FortiOS và FortiProxy;

Căn cứ Văn bản số 1559/CATTT-NCSC ngày 13/10/2022 của Cục An toàn thông tin về lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2022.

Qua công tác theo dõi, giám sát trên không gian mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin - Bộ Thông tin và Truyền thông cảnh báo:

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. Mức độ ảnh hưởng của lỗ hổng CVE-2022-40684 là nghiêm trọng. Việc rà soát và nâng cấp phiên bản hoặc áp dụng biện pháp khắc phục thay thế cần được thực hiện ngay lập tức.

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.

Nhằm đảm bảo an toàn thông tin cho hệ thống của các cơ quan, đơn vị, góp phần bảo đảm an toàn cho không gian mạng của tỉnh, Sở Giáo dục và Đào tạo yêu cầu các đơn vị triển khai thực hiện ngay một số nội dung sau:

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 *(danh sách lỗ hổng và hướng dẫn chi tiết tham khảo tại phụ lục kèm theo).*

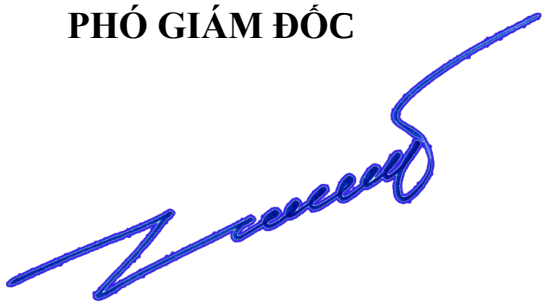
2. Tăng cường theo dõi giám sát hệ thống và có phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

Khi xảy ra sự cố liên quan đến an toàn, an ninh thông tin mạng và các hệ thống thông tin khác, liên hệ ông Nguyễn Hùng Cường - Chuyên viên phòng KTKĐCLGD&CNTT, Sở Giáo dục và Đào tạo theo số điện thoại 0968199100 để được hỗ trợ.

Nhận được văn bản này, Sở Giáo dục và Đào tạo yêu cầu Thủ trưởng các đơn vị nghiêm túc triển khai thực hiện./.

***Nơi nhận:***
- Như trên;
- Lãnh đạo Sở GDĐT;
- Lưu: VT, QLCL.

**KT.GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**



**Cù Huy Hoàn**

## PHỤ LỤC: THÔNG TIN LỖ HỔNG BẢO MẬT

### 1. Thông tin lỗ hổng bảo mật CVE-2022-40684

1.1. Lỗ hổng CVE-2022-40684

- 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.

1.2. 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.

1.3. 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-%20notes/289806/resolved-issues

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

### 2. Thông tin lỗ hổng bảo mật của Micorosoft

2.1. Thông tin các lỗ hổng

| TT | CVE | Mô tả | Link tham khảo |
|---|---|---|---|
| 1 | CVE-2022-41033 | -Điểm CVSS: 7.8 (Cao)<br>- 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.<br>- 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 |

| TT | CVE | Mô tả | Link tham khảo |
|---|---|---|---|
| 2 | CVE-2022-37987<br>CVE-2022-37989 | -Điểm CVSS: 7.8 (Cao)<br>- Lỗ hổng trong trong Windows Client Server Run-time Subsystem (CSRSS) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.<br>- 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<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37989 |
| 3 | CVE-2022-37968 | - Điểm CVSS: 10 (Nghiêm trọng)<br>- Lỗ hổng trong Azure Arc-enabled Kubernetes cluster Connect cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.<br>- Ảnh hưởng: Azure Stack Edge, Azure Arc-enabled Kubernetes cluster 1.6.19/1.5.8/1.7.18/1.8.11 | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37968 |
| 4 | CVE-2022-38048<br>CVE-2022-41043<br>CVE-2022-38001 | -Điểm CVSS: 7.8 (Cao)<br>- 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).<br>- Ảnh hưởng: Microsoft Office 2013/2016/2019, Office 365 Apps, Office LTSC. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38048<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41043<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38001 |

| TT | CVE | Mô tả | Link tham khảo |
|---|---|---|---|
| 5 | CVE-2022-41036<br>CVE-2022-41037<br>CVE-2022-41038 | Điểm CVSS: 8.8 (Cao)<br>- Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft SharePoint Server 2016/2019, SharePoint Foundation/Enterprise Server 2013. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41036<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41037<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41038 |
| 6 | CVE-2022-41031 | -Điểm CVSS: 7.8 (Cao)<br>- Lỗ hổng trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa.<br>- 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)<br>- Lỗ hổng trong Active Directory Certificate Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.<br>- Ảnh hưởng: Windows Server 2008/2012/2016/2019/ 2022 | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37976 |

2.2. 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. 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.

2.3. Nguồn 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