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

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

Số: 223 /TTCNTT-KTHT
V/v lỗ hổng bảo mật mới ảnh hưởng tới máy chủ thư điện tử sử dụng Zimbra

Hà Nội, ngày 10 tháng 08 năm 2021

Kính gửi: Các đơn vị trực thuộc Bộ có hệ thống thông tin

Trong tháng 7/2021, Zimbra đã phát hành bản vá cho 04 lỗ hổng bảo mật (CVE-2021-35208, CVE-2021-35209, CVE-2021-34807, CVE-2021-35207) trong sản phẩm của mình, trong đó đáng nổi bật là **02** lỗ hổng bảo mật **(CVE-2021-35208, CVE-2021-35209)** trong phần mềm Zimbra Collaboration (thông tin chi tiết lỗ hổng có tại Phụ lục kèm theo). Kết hợp các lỗ hổng này kẻ xấu không cần tài khoản đăng nhập hợp lệ vẫn có thể chiếm quyền điều khiển máy chủ Zimbra của tổ chức.

Zimbra Collaboration là một phần mềm nguồn mở máy chủ thư điện tử được sử dụng phổ biến, tại hơn 200.000 cơ quan, tổ chức, doanh nghiệp trên 160 quốc gia. Theo đánh giá sơ bộ của Cục An toàn thông tin, Việt Nam có trên 3.000 máy chủ thư điện tử sử dụng Zimbra đang được công khai trên Internet. Vì vậy, lỗ hổng bảo mật này có độ ảnh hưởng tương đối lớn, có thể dẫn đến các cuộc tấn công diện rộng.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Trung tâm Công nghệ thông tin khuyến nghị Quý đơn vị thực hiện:

1. Rà soát và khắc phục lỗ hổng bảo mật trên máy chủ thư điện tử của Quý đơn vị đặc biệt là lỗ hổng nói trên. Quý đơn vị nên cập nhật, nâng cấp lên phiên bản Zimbra mới nhất để khắc phục lỗ hổng bảo mật nói trên và các lỗ hổng bảo mật mới phát hiện khác.

2. Rà soát lại toàn bộ máy chủ thư điện tử và hệ thống liên quan để phát hiện và loại bỏ các tập tin độc hại có thể do đối tượng tấn công đã đưa lên hệ thống.

Trong trường hợp cần thiết, Quý đơn vị 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);
- Cổng thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

GIÁM ĐỐC

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

Hà Quốc Trung

Phụ lục
Thông tin lỗ hổng bảo mật
(Kèm theo Công văn số 223/TTCNTT-KTHT ngày 10 /08/2021 của Trung tâm Công nghệ thông tin)

1. Thông tin về các lỗ hổng

STT	CVE	Mô tả	Link tham khảo
1	CVE-2021-35208	- Lỗ hổng tồn tại trong ZmmailMsgView, cho phép đối tượng tấn công thực hiện tấn công giả mạo (XSS). - CVSS: 5.4 (trung bình) - Ảnh hưởng: phiên bản Zimbra Collaboration Suite 8.8 trước 8.8.15 và 9.x trước 9.0.0.	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories https://nvd.nist.gov/vuln/detail/CVE-2021-35208
2	CVE-2021-35209	- Lỗ hổng chuyển hướng mở trong Proxy Servlet. - CVSS: 6.1 (trung bình) - Ảnh hưởng: phiên bản Zimbra Collaboration Suite 8.8 trước 8.8.15 và 9.x trước 9.0.0.	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories https://nvd.nist.gov/vuln/detail/CVE-2021SS-35209
3	CVE-2021-34807	- Lỗ hổng chuyển hướng mở trong Proxy Servlet. - CVSS: 6.1 (trung bình) - Ảnh hưởng: Zimbra Collaboration Suite 8.8.x trước 8.8.15 và 9.0 trước 9.0.0.	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories https://nvd.nist.gov/vuln/detail/CVE-2021-34807
4	CVE-2021-35207	- Lỗ hổng tồn tại trong Zimbra Collaboration, cho phép đối tượng tấn công thực hiện tấn công giả mạo (XSS). - CVSS: 6.1 (trung bình) - Ảnh hưởng: Zimbra Collaboration Suite 8.8.x trước 8.8.15 và 9.0 trước 9.0.0.	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories https://nvd.nist.gov/vuln/detail/CVE-2021-35207

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục các lỗ hổng bảo mật này là nâng cấp bản vá tương ứng theo hướng dẫn của hãng. Thông tin tham khảo có tại: https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

Hiện tại hãng chưa có biện pháp khắc phục giảm thiểu nguy cơ tấn công vì vậy Quý đơn vị cần nâng cấp bản vá trong thời gian sớm nhất.

3. Nguồn tham khảo

https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

DANH SÁCH CÁC ĐƠN VỊ CÓ HỆ THỐNG CNTT

(Kèm theo Công văn số 223/TTCNTT-KTHT ngày 10/08/2021 của Trung tâm Công nghệ thông tin)

TT	Tên đơn vị
1.	Tổng cục Tiêu chuẩn Đo lường Chất lượng
2.	Cục Thông tin Khoa học và Công nghệ Quốc gia
3.	Cục An toàn bức xạ và hạt nhân
4.	Cục Sở hữu trí tuệ
5.	Ban quản lý khu công nghệ cao Hoà Lạc
6.	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
7.	Viện Năng lượng nguyên tử Việt Nam
8.	Viện Khoa học sở hữu trí tuệ
9.	Quỹ Phát triển khoa học và công nghệ quốc gia
10.	Quỹ Đổi mới công nghệ quốc gia