UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 615 /STTTT-TTGSĐH
Về việc cảnh báo lỗ hổng bảo mật Spring4Shell, CVE-2022-29464 và trong các sản phẩm Microsoft công bố tháng 4/2022.

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

Tây Ninh, ngày 27 tháng 4 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 508/CATTT-NCSC, Công văn số 430/CATTT-NCSC, Công văn số 548/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 TRONG CÁC SẢN PHẨM MICROSOFT CÔNG BỐ THÁNG 4/2022

1. Lỗ hổng bảo mật CVE-2022-29464

- Mô tả:

Lỗ hổng ảnh hưởng đến sản phẩm WSO2 cho phép đối tượng tấn công thực thi mã từ xa trên máy chủ.

- **CVSS: 9.8** (Nghiêm trọng).

- **Ảnh hưởng**:

WSO2 API Manager phiên bản 2.2.0 trở lên;

WSO2 Identity Server phiên bản 5.2.0 trở lên;

WSO2 Identity Server Analytics phiên bản 5.4.0, 5.4.1, 5.5.0, 5.6.0;

WSO2 Identity Server as Key Manager phiên bản 5.3.0 trở lên;

WSO2 Enterprise Integrator phiên bản 6.2.0 trở lên.

- Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục lỗ hổng này là nâng cấp lên phiên bản mới nhất. Trong trường hợp không thể nâng cấp do chưa có phát hành phiên bản mới tương ứng với phiên bản đang sử dụng, Quý đơn vị có thể áp dụng các bản sửa lỗi liên quan dựa trên các bản sửa lỗi đã công khai được cung cấp dưới đây:

https://github.com/wso2/carbon-kernel/pull/3152

https://github.com/wso2/carbon-identity-framework/pull/3864

https://github.com/wso2-extensions/identity-carbon-auth-rest/pull/167

Ngoài ra để giảm thiểu nguy cơ tấn công, Quý đơn vị có thể thực hiện các bước khắc phục thay thế tạm thời như sau:

Phiên bản bị ảnh hưởng	Các bước khắc phục thay thế
WSO2 API Manager 2.6.0, 2.5.0, 2.2.0 WSO2 Identity Server 5.8.0, 5.7.0, 5.6.0, 5.5.0, 5.4.1, 5.4.0, 5.3.0, 5.2.0 WSO2 Identity Server as Key Manager 5.7.0, 5.6.0, 5.5.0, 5.3.0 WSO2 IS Analytics 5.6.0, 5.5.0, 5.4.1, 5.4.0	Xóa tất cả mapping defined bên trong FileUploadConfig tag tại: /repository/conf/carbon.xml

<table>
<tr>
<td>WSO2 API Manager 4.0.0, 3.2.0, 3.1.0, 3.0.0</td>
<td>Thêm cấu hình dưới đây vào /repository/conf/deployment.toml
deployment.toml
[[resource.access_control]]
context="(.*)/fileupload/resource(.*)"
secure=false http_method = "all"
[[resource.access_control]]
context="(.*)/fileupload/(.*)"
secure=true http_method = "all"
permissions = ["/permission/protected/"]</td>
</tr>
<tr>
<td>WSO2 Identity Server 5.11.0, 5.10.0, 5.9.0 WSO2 Identity Server as Key Manager 5.10.0, 5.9.0</td>
<td>Thêm cấu hình dưới đây vào /repository/conf/deployment.toml
deployment.toml
[[resource.access_control]]
context="(.*)/fileupload/service(.*)"
secure=false http_method = "all"
[[resource.access_control]]
context="(.*)/fileupload/entitlement-policy(.*)" secure=false http_method = "all" [[resource.access_control]]
context="(.*)/fileupload/resource(.*)"
secure=false http_method = "all"
[[resource.access_control]]
context="(.*)/fileupload/(.*)"
secure=true http_method = "all"
permissions = ["/permission/protected/"]</td>
</tr>
<tr>
<td>WSO2 Enterprise Integrator 6.6.0, 6.5.0, 6.4.0, 6.3.0, 6.2.0</td>
<td>Đối với EI profile, xóa mappings trong tệp /conf/carbon.xml ra khỏi Đối với Business process / Broker và Analytics profiles, thay đổi lại tệp carbon.xml cho các vị trí tương ứng sau:
/wso2/broker/conf/carbon.xml
/wso2/businessprocess/conf/carbon.xml
/wso2/anlalytics/conf/carbon.xm</td>
</tr>
</table>

- Nguồn tham khảo: Security Advisory WSO2-2021-1738 - WSO2 Platform Security - WSO2 Documentation

2. Lỗ hổng bảo mật Spring4Shell

- Mô tả: Lỗ hổng này tồn tại trong Spring Core, cho phép đối tượng tấn công thực thi mã từ xa.

- Ảnh hưởng: ứng dụng sử dụng Spring Core phiên bản JDK >= 9.0

- Hướng kiểm tra và khắc phục:

Bước 1: Kiểm tra phiên bản JDK

Trên máy chủ, hãy chạy lệnh "java -version" để kiểm tra phiên bản JDK đang chạy. Nếu phiên bản <= 8.0, hệ thống Quý đơn vị không bị ảnh hưởng bởi lỗ hổng này.

Bước 2: Kiểm tra việc sử dụng Spring Framework

Đối với hệ thống được triển khai dưới dạng war package:

- Giải nén war package

- Tìm kiếm tệp jar ở định dạng spring-beans-*.jar (ví dụ: spring-beans 5.3.16.jar) trong tệp giải nén. Nếu có tồn tại, nghĩa là hệ thống đang sử dụng Spring framework.

Đối với hệ thống được triển khai dưới dang jar package:

- Giải nén jar package

- Tìm kiếm tệp jar ở định dạng **spring-beans-*.jar** (ví dụ: spring-beans 5.3.16.jar) trong tệp giải nén. Nếu có tồn tại, nghĩa là hệ thống đang sử dụng Spring framework.

- Nếu không tìm thấy tệp **spring-beans-*.jar**, hãy tiếp tục tìm kiếm tệp CachedIntrospectionResults.class trong tệp giải nén. Nếu tồn tại tệp này chứng tỏ hệ thống đang sử dụng Spring framework.

Bước 3: Phân tích, điều tra xác nhận 4 Sau khi hoàn thành 2 bước kiểm tra ở trên, các điều kiện sau được đáp ứng đồng thời sẽ xác định hệ thống bị ảnh hưởng bởi lỗ hổng bảo mật này:

- Phiên bản JDK >= 9.0

- Sử dụng Spring framework hoặc derived framework.

- Tồn tại endpoint sử dụng chức năng DataBinder.

Hướng dẫn khắc phục

Hiện tại, chưa có bản vá để khắc phục lỗ hổng bảo mật nói trên. Vì vậy, để giảm thiểu nguy cơ bị tấn công, Quý đơn vị có thể thực hiện các biện pháp khắc phục theo nguồn hướng dẫn tham khảo của một số tổ chức tại: https://www.cyberkendra.com/2022/03/springshell-rce-0-dayvulnerability.html

Nguồn tham khảo

https://www.cyberkendra.com/2022/03/springshell-rce-0-dayvulnerability.html

https://www.cyberkendra.com/2022/03/spring4shell-details-and-exploitcode.ht

3. Các lỗ hổng bảo mật có mức ảnh hưởng Nghiêm trọng được Microshoft công bố trong ngày 12/4/2022:

Mô tả

- Lỗ hổng bảo mật CVE-2022-26809 trong RPC Runtime Library cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao trên hệ thống bị ảnh hưởng.
- 02 lỗ hổng bảo mật CVE-2022-24491, CVE-2022-24497 trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao.

Các lỗ hổng bảo mật có mức ảnh hưởng Cao:

- Lỗ hổng bảo mật CVE-2022-26815 trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng bảo mật CVE-2022-26904 trong Windows User Profile Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đã có mã khai thác công khai trên Internet.
- Lỗ hổng bảo mật CVE-2022-26919 trong Windows LDAP cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng bảo mật CVE-2022-24521 trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền

Thông tin chi tiết về các lỗ hổng

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-26809	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong RPC Runtime Library cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao trên hệ thống bị ảnh hưởng. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE2022-26809
2	CVE-2022-24497	- Điểm CVSS: 7.2 (cao) - Lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CV E-2022-24491

		- Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022.	
3	CVE-2022-24497	- 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 8.1/10, Windows Server 2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CV E-2022-24497
4	CVE-2022-26815	- Điểm CVSS: 7.2 (cao) - Lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26815
5	CVE-2022-26904	- Điểm CVSS: 8.1 (Cao) - Lỗ hổng trong Windows LDAP cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CV E-2022-26919
6	CVE-2022-26919	- Điểm CVSS: 8.1 (Cao) - Lỗ hổng trong Windows LDAP cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CV E-2022-26919

7	CVE-2022-24521	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Common Log File System Driver 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/en-US/vulnerability/CVE-2022-24521

Hướng 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:

1. April 2022 Security Updates - Release Notes - Security Update Guide - Microsoft
2. Zero Day Initiative — The April 2022 Security Update Review