

UBND TỈNH TÂY NINH  
**SỞ THÔNG TIN VÀ TRUYỀN THÔNG**

Số: /STTTT-TTGSĐH  
V/v cảnh báo và khắc phục lỗ hổng bảo mật  
HĐH Window và Oracle Weblogic Server

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

Tây Ninh, ngày tháng 9 năm 2021

Kính gửi:

- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các Sở, ban, ngành tỉnh;
- UBND các huyện, thị xã, thành phố.

Thực hiện theo Công văn số 984/CATTT-NCSC của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật mới ảnh hưởng đến hệ điều hành Windows 10, Windows Server (**CVE-2021-36934**) và Công văn số 993/CATTT-NCSC về việc cảnh báo 06 lỗ hổng bảo mật mới ảnh hưởng cao và nghiêm trọng trong Oracle WebLogic Server (**CVE-2021-2394, CVE-2021-2397, CVE-2021-2382, CVE-2021-2378, CVE-2021-2376, CVE-2021-2403**).

Để 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. Rà soát, kiểm tra cho các máy tính/máy chủ nếu nằm trong phạm vi ảnh hưởng của lỗ hổng bảo mật và tiến hành khắc phục (*Phụ lục hướng dẫn kèm theo*).
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 - Phó Giám đốc Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0932624462.

Trân trọng./.

**Nơi nhận:**

- Như trên;
- Lưu: VT, TTGSĐH.

**KT. GIÁM ĐỐC  
PHÓ GIÁM ĐỐC**

# PHỤ LỤC I

## HƯỚNG DẪN KHẮC PHỤC LỖ HỔNG BẢO MẬT

### CVE-2021-36934

#### 1. Thông tin lỗ hổng bảo mật

Lỗ hổng bảo mật **CVE-2021-36934** tồn tại do các tài khoản người dùng thường có thể truy cập vào các tệp hệ thống (như các tệp SAM, Windows Registry). Khai thác thành công lỗ hổng này, cho phép đối tượng tấn công thực thi mã tùy ý với đặc quyền cao hơn trên hệ thống mục tiêu. Cho đến thời điểm này theo công bố của Microsoft xác nhận rằng lỗ hổng này ảnh hưởng đến hệ điều hành Windows 10 phiên bản 1809/1909/2004/21H1/20H2, Windows Server 2019/20H2.

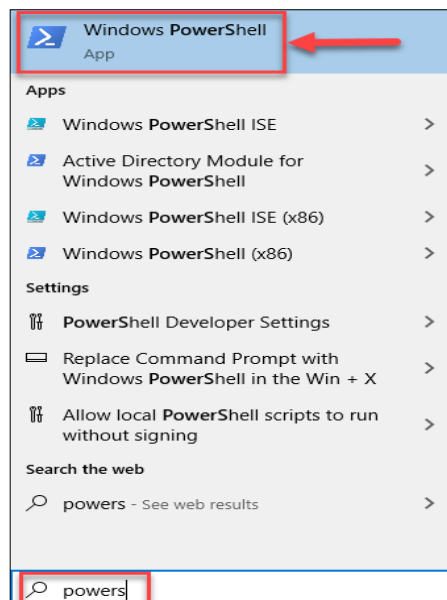
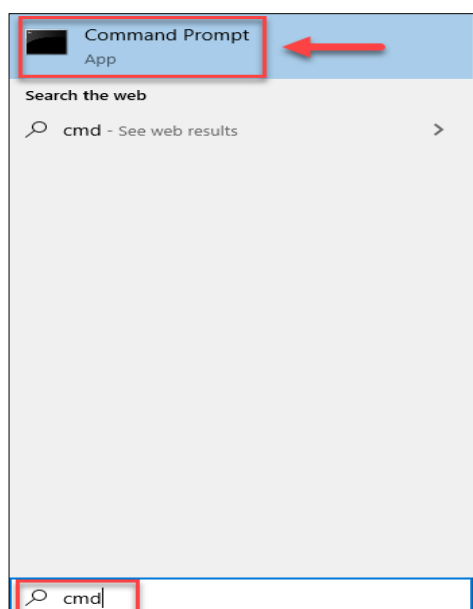
#### 2. Hướng dẫn khắc phục

Microsoft chưa có thông tin phát hành bản vá cho lỗ hổng này, thay vào đó là đưa ra biện pháp khắc phục thay thế để giảm thiểu nguy cơ tấn công. Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) khuyến nghị nên thực hiện một số biện pháp như sau:

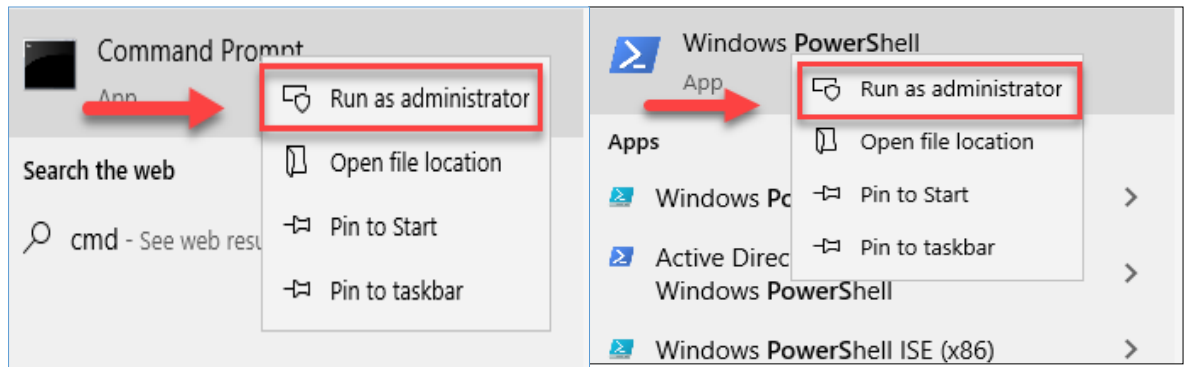
- **Bước 1:** Đối với các máy tính sử dụng hệ điều hành trong danh sách tại mục 2.1

+ Mở *Command Prompt* hoặc *Windows PowerShell* bằng quyền *Admin*

+ Trên thanh **Start** > nhập **cmd** hoặc **powershell**



+ Chuột phải chọn **Run as administrator** > chọn **YES** khi có bảng thông báo hiện ra



+ Kiểm tra máy tính có bị ảnh hưởng lỗ hổng CVE-2021-36934, trên Command Prompt hoặc Windows PowerShell, sử dụng lệnh:

```
icacls C:\Windows\System32\config\sam
```

+ Nếu hiển thị **BUILTIN\Users:(I)(RX)**, máy tính bị ảnh hưởng bởi lỗ hổng. Thực hiện tiếp các bước sau để khắc phục lỗ hổng.

+ Nếu không hiển thị lỗi như hình dưới đây, máy tính không bị ảnh hưởng và không cần thực hiện các bước tiếp theo

-Trên giao diện Command Prompt:

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>icacls C:\Windows\System32\config\sam
C:\Windows\System32\config\sam BUILTIN\Administrators:(I)(F)
                                NT AUTHORITY\SYSTEM:(I)(F)
                                BUILTIN\Users:(I)(RX)
                                APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
                                APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(RX)
```

- Trên giao diện Windows PowerShell

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> icacls C:\Windows\System32\config\sam
C:\Windows\System32\config\sam BUILTIN\Administrators:(I)(F)
                                NT AUTHORITY\SYSTEM:(I)(F)
                                BUILTIN\Users:(I)(RX)
                                APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
                                APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(RX)

Successfully processed 1 files; Failed processing 0 files
```

Nếu kết quả nhận được giống như thông tin theo ảnh ở trên thì máy tính đang bị ảnh hưởng bởi lỗ hổng **CVE-2021-36934**, Quý đơn vị tiến hành khắc phục tạm thời theo hướng dẫn các bước tiếp theo.

**Bước 2:** Sử dụng lệnh để hạn chế quyền truy cập vào thư mục **%windir%\system32\config**

➤ Trên giao diện Command Prompt:



- **Bước 3:** Kiểm tra lại quyền thư mục như ở **Bước 1:**

➤ **Trên giao diện Command Prompt**

```

C:\Users\ADMIN>icacls C:\Windows\System32\config\sam
C:\Windows\System32\config\sam NT AUTHORITY\SYSTEM:(I)(F)
                        BUILTIN\Administrators:(I)(F)
                        DESKTOP-OI9KF0T\ADMIN:(I)(F)

Successfully processed 1 files; Failed processing 0 files

C:\Users\ADMIN>

```

➤ **Trên giao diện Windows PowerShell**

```

Administrator: Windows PowerShell
Successfully processed 1 files; Failed processing 0 files
PS C:\Windows\system32> ^C
PS C:\Windows\system32> ^C
PS C:\Windows\system32> icacls C:\Windows\System32\config\sam
C:\Windows\System32\config\sam NT AUTHORITY\SYSTEM:(I)(F)
                        BUILTIN\Administrators:(I)(F)
                        DESKTOP-OI9KF0T\ADMIN:(I)(F)

Successfully processed 1 files; Failed processing 0 files
PS C:\Windows\system32>

```

**Bước 4:** Xóa các bản sao của Volume Shadow Copy Service, System Restore (nếu có)

**Lưu ý:** Việc thực hiện xóa Shadow Copy có thể ảnh hưởng đến hoạt động khôi phục, bao gồm khả năng khôi phục dữ liệu bằng các ứng dụng sao lưu của bên thứ ba.

➤ **Cách 1:** Sử dụng lệnh trên Command Prompt

-Hiển thị tất cả các bản sao lưu Shadow Copy:

```
vssadmin list shadows /for=%systemdrive%
```

```

C:\Windows\system32>vssadmin list shadows /for=%systemdrive%
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Contents of shadow copy set ID: {8175d0db-f205-4fb0-85f7-7156ff095b56}
  Contained 1 shadow copies at creation time: 7/21/2021 8:28:45 PM
  Shadow Copy ID: {79f56c3e-6c83-4574-9c8d-7db59b8b0b4d}
  Original Volume: (C:)\\?\Volume{ace2b02b-0000-0000-0000-300300000000}\
  Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy5
  Originating Machine: DESKTOP-OI9KF0T.test2019.local
  Service Machine: DESKTOP-OI9KF0T.test2019.local
  Provider: 'Microsoft Software Shadow Copy provider 1.0'
  Type: ClientAccessibleWriters
  Attributes: Persistent, Client-accessible, No auto release, Differential, Auto recovered

Contents of shadow copy set ID: {26e1703c-b129-4e8b-ac1e-ee4cf48a87c9}
  Contained 1 shadow copies at creation time: 7/21/2021 8:28:57 PM
  Shadow Copy ID: {6c234981-277b-4ec3-873c-769bb8d8653f}
  Original Volume: (C:)\\?\Volume{ace2b02b-0000-0000-0000-300300000000}\
  Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6
  Originating Machine: DESKTOP-OI9KF0T.test2019.local
  Service Machine: DESKTOP-OI9KF0T.test2019.local
  Provider: 'Microsoft Software Shadow Copy provider 1.0'
  Type: ClientAccessibleWriters
  Attributes: Persistent, Client-accessible, No auto release, Differential, Auto recovered

```



- Xóa toàn bộ các bản sao lưu:

```
vssadmin delete shadows /for=%systemdrive% /Quiet
```

```
C:\Windows\system32>vssadmin delete shadows /for=%systemdrive% /Quiet
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.
```

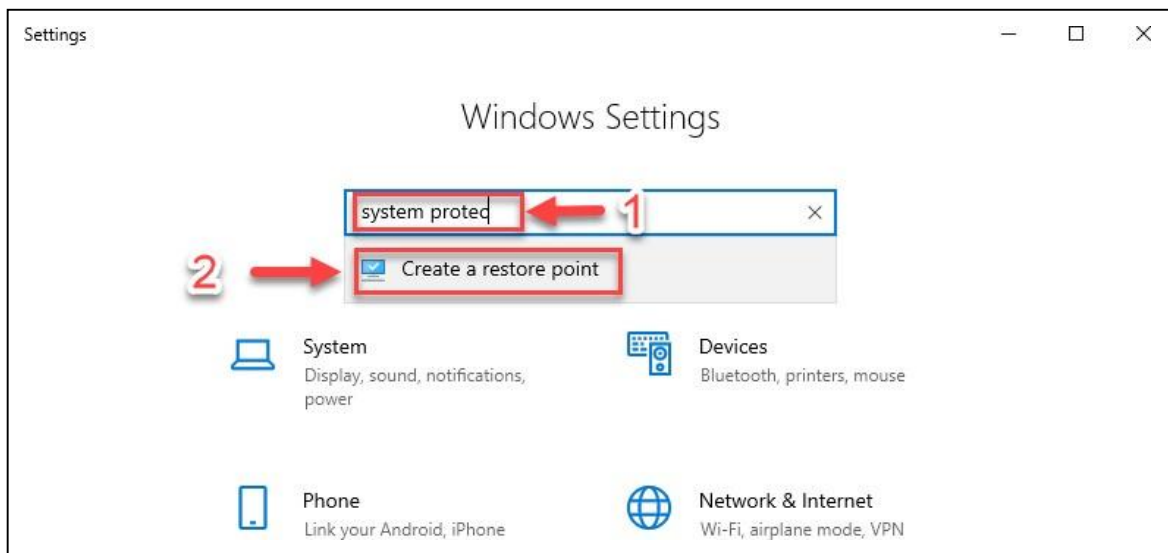
- **Kiểm tra lại các bản sao lưu đã bị xóa hay chưa:**

```
vssadmin list shadows /for=%systemdrive%
```

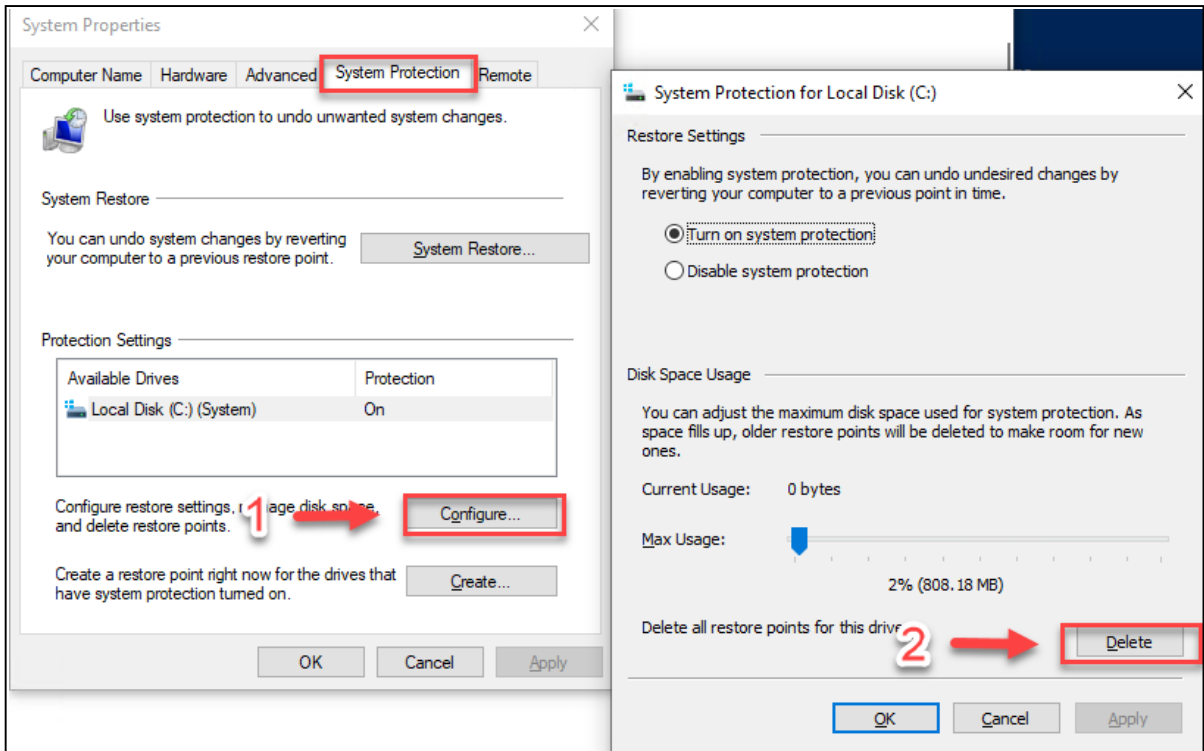
```
C:\Windows\system32>vssadmin list shadows /for=%systemdrive%
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.
No items found that satisfy the query
```

➤ **Cách 2:** Sử dụng giao diện

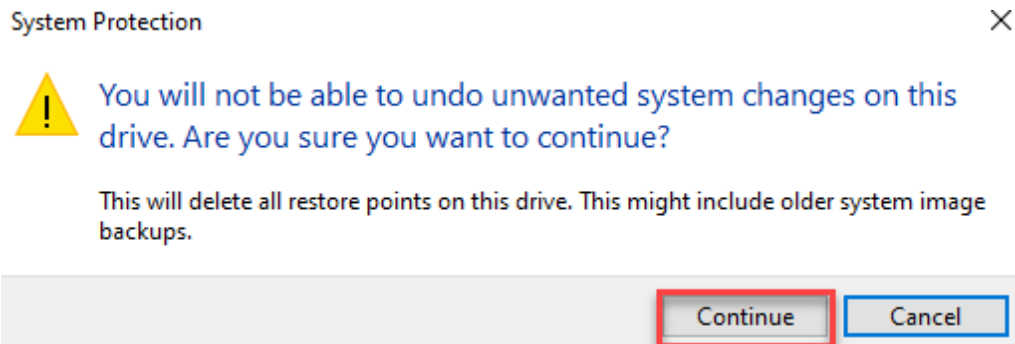
- Truy cập **Setting** > nhập vào ô tìm kiếm **System protect** > Chọn mục **Create a restore point**



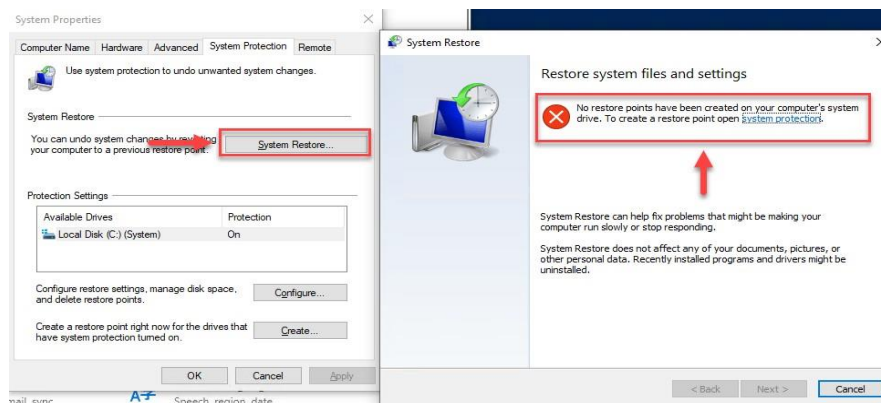
- Tại tab **System Protection** > Chọn **Configure** > chọn **Delete** tại **Delete all restore points for this drive** trên cửa sổ pop-up mới hiện lên



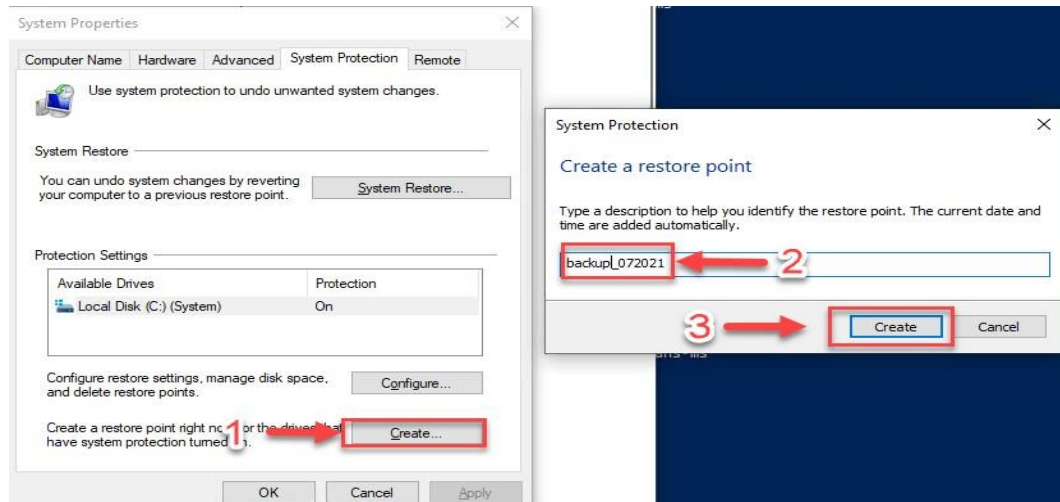
-Chọn **Continue** để hoàn tất việc xóa các bản sao



-**Kiểm tra các bản sao lưu đã được xóa:** Tại tab **System Protection** > Chọn System Restore



**-Tạo bản sao lưu mới (nếu cần):** Tại tab **System Protection** > Chọn **Create**



### 3. Tài liệu tham khảo

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934>



**PHỤ LỤC II**  
**HƯỚNG DẪN KHẮC PHỤC LỖ HỔNG BẢO MẬT**  
**ORACLE WEBLOGIC**

**I. Thông tin lỗ hổng bảo mật**

Lỗ hổng bảo mật **CVE-2021-2394, CVE-2021-2397, CVE-2021-2382, CVE-2021-2378, CVE-2021-2376, CVE-2021-2403**, trong đó **03** lỗ hổng bảo mật (**CVE-2021-2394, CVE-2021-2397, CVE-2021-2382**) có mức ảnh hưởng nghiêm trọng, cho phép đối tượng tấn công thực thi mã từ xa mà không cần xác thực nhằm chiếm quyền điều khiển máy chủ.

<b>TT</b>	<b>CVE</b>	<b>Mô tả</b>	<b>Link tham khảo</b>
<b>1</b>	CVE-2021-2394	Lỗ hổng trong Oracle WebLogic Server, cho phép đối tượng tấn công truy cập trái phép, từ đó chiếm quyền điều khiển máy chủ mục tiêu.  Điểm CVSS: 9,8 (nghiêm trọng)	<a href="https://www.oracle.com/security-alerts/cpu-jul2021.html">https://www.oracle.com/security-alerts/cpu-jul2021.html</a>  <a href="https://nvd.nist.gov/vuln/detail/CVE-2021-2394">https://nvd.nist.gov/vuln/detail/CVE-2021-2394</a>
<b>2</b>	CVE-2021-2397	Lỗ hổng trong Oracle WebLogic Server, cho phép đối tượng tấn công truy cập trái phép, từ đó chiếm quyền điều khiển máy chủ mục tiêu.  Điểm CVSS: 9,8 (nghiêm trọng)	<a href="https://www.oracle.com/security-alerts/cpu-jul2021.html">https://www.oracle.com/security-alerts/cpu-jul2021.html</a>  <a href="https://nvd.nist.gov/vuln/detail/CVE-2021-2397">https://nvd.nist.gov/vuln/detail/CVE-2021-2397</a>
<b>3</b>	CVE-2021-2382	Lỗ hổng trong Oracle WebLogic Server, cho phép đối tượng tấn công truy cập trái phép, từ đó chiếm quyền điều khiển máy chủ mục tiêu.  Điểm CVSS: 9,8 (nghiêm trọng)	<a href="https://www.oracle.com/security-alerts/cpu-jul2021.html">https://www.oracle.com/security-alerts/cpu-jul2021.html</a>  <a href="https://nvd.nist.gov/vuln/detail/CVE-2021-2382">https://nvd.nist.gov/vuln/detail/CVE-2021-2382</a>
<b>4</b>	CVE-2021-2378	Lỗ hổng trong Oracle WebLogic Server, cho phép đối tượng tấn công truy cập trái phép máy chủ mục tiêu.  Điểm CVSS: 7.5 (cao)	<a href="https://www.oracle.com/security-alerts/cpu-jul2021.html">https://www.oracle.com/security-alerts/cpu-jul2021.html</a>  <a href="https://nvd.nist.gov/vuln/detail/CVE-2021-2378">https://nvd.nist.gov/vuln/detail/CVE-2021-2378</a>
<b>5</b>	CVE-2021-2376	Lỗ hổng trong Oracle WebLogic Server, cho phép đối tượng tấn công truy cập trái phép máy chủ	<a href="https://www.oracle.com/security-alerts/cpu-jul2021.html">https://www.oracle.com/security-alerts/cpu-jul2021.html</a>  <a href="https://nvd.nist.gov/vuln/">https://nvd.nist.gov/vuln/</a>

		mục tiêu. Điểm CVSS: 7.5 (cao)	de- tail/CVE-2021-2376
6	CVE-2021-2403	Lỗ hổng trong Oracle WebLogic Server, cho phép đối tượng tấn công truy cập trái phép máy chủ mục tiêu. Điểm CVSS: 5.3 (trung bình)	<a href="https://www.oracle.com/security-alerts/cpujul2021.html">https://www.oracle.com/security-alerts/cpujul2021.html</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-2021-2403">https://nvd.nist.gov/vuln/detail/CVE-2021-2403</a>

## 2. Hướng dẫn khắc phục

Cách tốt nhất để khắc phục các lỗ hổng bảo mật này là cập nhật bản vá theo hướng dẫn của Oracle. Tại thời điểm này, Oracle chưa có công bố về các biện pháp khắc phục thay thế để giảm thiểu nguy cơ tấn công.

Vì vậy, đơn vị cần thực hiện cập nhật bản vá trong thời gian sớm.

## 3. Tài liệu tham khảo

<https://www.oracle.com/security-alerts/cpujul2021.html>