



VIII FORUM KIEROWNIKÓW IT W ADMINISTRACJI

 24-26.04.2023

 ZAKOPANE
BACHLEDA HOTEL KASPROWY

 forum.itwadministracji.pl



Oczami administratora i użytkownika: wyzwania i rozwiązania dotyczące podatności systemów informatycznych w administracji publicznej



Prowadzący: Kamil Strzałka

Gra w Zero-Day'e

80%

Taka ilość podatności ma przygotowany gotowy exploit zanim pojawi się na nią łatka



Gra w Zero-Day'e

60 do 150 dni

Tyle dni statystycznie zajmuje zespołowi IT zanim rozdystrybuuje patch na urządzenia. Minimum 38 zajmuje przygotowanie do tego zadania



CVE-2021-44228

- **Data Publikacji:**
12/10/2021
- **CVSS: 10.0 CRITICAL**
- **Wektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
- <https://www.cvedetails.com/cve/CVE-2021-44228/>



Gra w Zero-Day'e

social engineering

Najślabszym ogniwem jest tu użytkownik

VIII FORUM
KIEROWNIKÓW IT
W ADMINISTRACJI



Zabezpieczenia



Szybko czy dokładnie ?

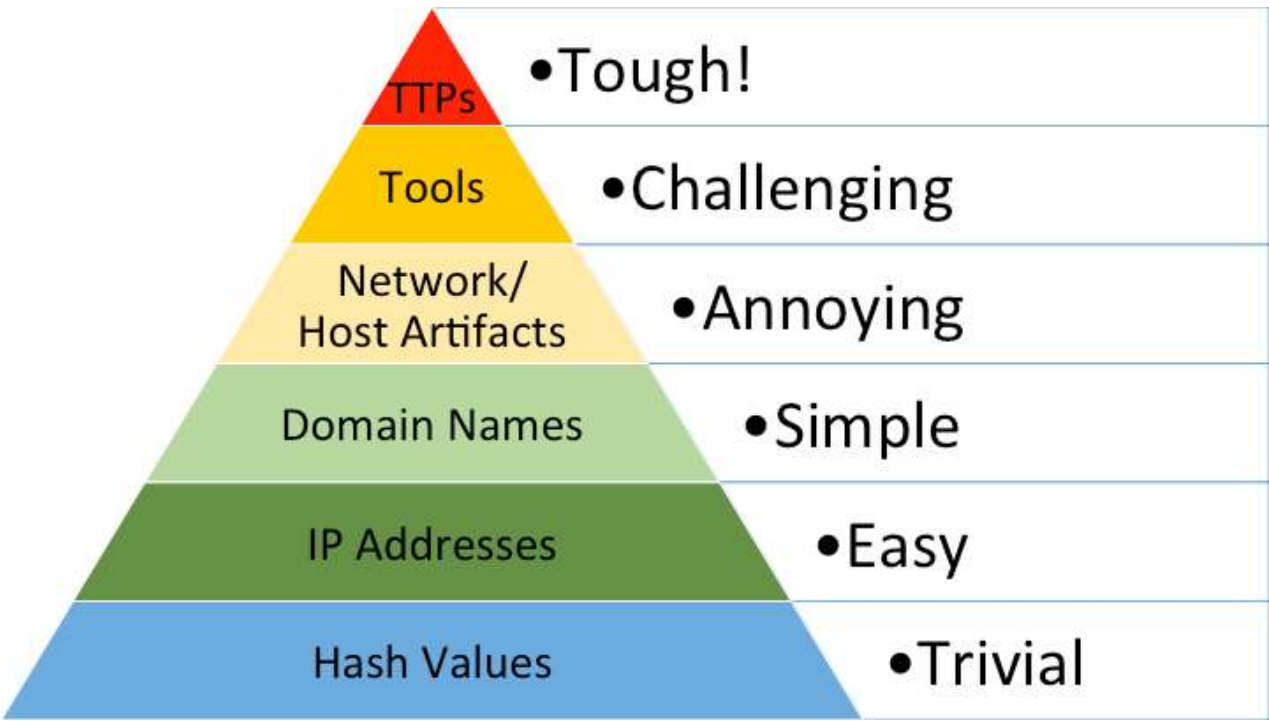
Discovery Scanning

Full Scanning

Compliance Scanning



Piramida Bólu



„Zaszczytne” drugie miejsce

22%

Podatności windows to druga w kolejności technologia pod względem powstających exploitów (lata 2000-2022)



Patchowanie wystarczy ?

60%

W 60% przypadków patch powstaje 1-2 tygodnie po wydaniu expolita



To ile tych podatności?



Głosowanie <https://www.menti.com/al7dgv3kki9b>



To ile tych podatności?



Wyniki



<https://www.mentimeter.com/app/presentation/alp72pjmm9w9q4g2514hjwz2zfmcsxy>










Badane Środowisko































- Podstawowa konfiguracja
- Windows 11 PRO 22H2
- Aplikacje: 7zip, Office, Adobe
- Office Semi-Annual Enterprise Channel
- Wersja - 15601.20538



Badane Środowisko

Software

<input type="checkbox"/>	Name ▲	Vendor		Version
1	 .Net Framework	Microsoft		4.8.1-en
2	 .Net Framework	Microsoft		4.7.2-en
3	 7-Zip	Igor Pavlov		22.01-x64
4	 Aplikacje Microsoft 365 dla przedsiębiorstw - pl-pl	Microsoft Corporation		16.0.15601.20538
5	 Aplikacje Microsoft 365 dla przedsiębiorstw - pl-pl.proof	Microsoft Corporation		16.0.15601.20538
6	 baramundi Management Agent	baramundi software AG		22.2.205.0
7	 Edge	Microsoft		110.0.1587.57
8	 Edge WebView 2	Microsoft		110.0.1587.57
9	 Microsoft Office 365 - PoC	Microsoft Corporation		16.x
10	 Microsoft OneDrive	Microsoft Corporation		22.077.0410.0007
11	 Microsoft Update Health Tools	Microsoft Corporation		5.69.0.0
12	 Office 365	Microsoft Corporation		16.0.15601.20538-x64-SAEC
13	 Reader	Adobe		2022.003.20322-mui
14	 Windows 10 Pro	Microsoft Corporation		10.0 22621 x64 pl-PL
15	 Windows 11 22H2	Microsoft		



Badane Środowisko

Microsoft Update

Update download mode	HTTP only
Update profile	Windows Endpoints - Test Environment - testowe
Update state	✓
Last successful update	5 hours ago (2/27/2023 8:05 PM) / Microsoft Update Online
Last inventory	5 hours ago (2/27/2023 8:06 PM) / Microsoft Update Online
Missing updates	none found





Wyniki

Detected

	CVE ID	CVSS 9
1	🚩 CVE-2022-30188	6.8
2	🚩 CVE-2022-29119	6.8
3	🚩 CVE-2022-29111	6.8
4	🚩 CVE-2022-22018	6.8

Overview

Risk level 

Vulnerabilities found 

22018

[/M-1-EC \(BARTOSZ\)](#)

High threat 0 (0%)

Medium threat

HIGH Microsoft Windows HEVC Video Extensions Remote Code Execution (June 2022)

Description

The Windows 'HEVC Video Extensions' or 'HEVC from Device Manufacturer' app installed on the remote host is affected by a remote code execution vulnerability. An attacker who successfully exploits these vulnerabilities could execute arbitrary code. Exploitation of the vulnerability requires that a program process a specially crafted file.

```
\\Microsoft.HEVCVideoExtension_8wekyb3d8bbwe\
```



Szybkie rozwiązania

```
Administrator: Windows PowerShell  
Microsoft.RawImageExtension  
Microsoft.WindowsMaps  
Microsoft.WindowsSoundRecorder  
Microsoft.Getstarted  
Microsoft.WindowsCamera  
Microsoft.WindowsFeedbackHub  
Microsoft.WindowsNotepad  
Microsoft.MicrosoftStickyNotes  
Microsoft.MicrosoftOfficeHub  
Microsoft.DesktopAppInstaller
```

```
Administrator: Windows PowerShell  
PS C:\Windows\system32> remove-appxpackage Microsoft.HEVCVideoExtension_1.0.50361.0_x64__8wekyb3d8bbwe_  
Microsoft.Windows.Photos  
Microsoft.GetHelp  
Microsoft.WindowsTerminal  
Microsoft.XboxGamingOverlay  
MicrosoftCorporationII.QuickAssist  
microsoft.windowscommunicationsapps  
Microsoft.Todos  
Microsoft.PowerAutomateDesktop  
Microsoft.MicrosoftSolitaireCollection  
Microsoft.WindowsAppRuntime.1.2  
Microsoft.WindowsAppRuntime.1.2  
Microsoft.YourPhone  
Microsoft.LanguageExperiencePackpl-PL  
PS C:\Windows\system32> remove-appxpackage Microsoft.HEVCVideoExtension_
```



Szybkie rozwiązania

baramundi OS Customization Tool

Overview

Features

Apps

Patches

Settings

Corporate Design

Privacy

Summary

Apps

To remove an app clear its checkbox. Once Apps are removed from an image, they cannot be re-added.

Select all


- Clipchamp.Clipchamp
- Microsoft.S49981C3F5F10
- Microsoft.BingNews
- Microsoft.BingWeather
- Microsoft.DesktopAppInstaller
- Microsoft.GamingApp
- Microsoft.GetHelp
- Microsoft.Getstarted
- Microsoft.HEIFImageExtension
- Microsoft.HEVCVideoExtension**
- Microsoft.MicrosoftOfficeHub
- Microsoft.MicrosoftSolitaireCollection
- Microsoft.MicrosoftStickyNotes
- Microsoft.Paint
- Microsoft.People
- Microsoft.PowerAutomateDesktop
- Microsoft.RawImageExtension
- Microsoft.ScreenSketch
- Microsoft.SecHealthUI
- Microsoft.StorePurchaseApp








Zostaje jeszcze konfiguracja

Standard



 Filter entries

<input type="checkbox"/>	CCE ID	Severity ▼	Checked	Title	Scan profile
1	 CCE-8825-2	Medium	4 hours ago	The Windows SMB server is not enabled to perform SMB packet signing when...	Configuration Scan:
2	 CCE-9344-3	Medium	4 hours ago	The Windows SMB client is not enabled to perform SMB packet signing when...	Configuration Scan:
3	 CCE-9040-7	Medium	4 hours ago	The Windows SMB server is not enabled to always perform SMB packet signing.	Configuration Scan:
4	 CCE-9265-0	Medium	4 hours ago	Unencrypted password is sent to third-party SMB server.	Configuration Scan:
5	 CCE-9327-8	Medium	4 hours ago	The Windows SMB client is not enabled to always perform SMB packet signing.	Configuration Scan:



„Zero” da się uzyskać...

Risk level



[0 vulnerabilities found \(therefrom 0 severe\)](#)

Vulnerabilities found



-  High threat
-  Medium threat
-  Low threat

ale tylko w próżni!



W praktyce:

Overview

Risk level



[92 vulnerabilities found \(therefrom 67 severe\)](#)

Vulnerabilities found



- High threat: 67 (73%)
- Medium threat: 25 (27%)
- Low threat: 0 (0%)

Top 5 vulnerabilities

- 9.8** [CVE-2022-23521](#)
Integer overflow vulnerability in Git via a crafted .gitattributes file - C...
- CVSS Version: 3.1
11 hours ago
- 9.8** [CVE-2022-41903](#)
Heap overflow vulnerability in Git via the export-subst mechanism - C...

[92 vulnerabilities found](#)

Top 5 vulnerable products

- 9.8** [Microsoft 365 Apps for Enterprise](#)
9 vulnerabilities
- 9.8** [Git](#)
3 vulnerabilities
- 9.8** [Microsoft Word, Microsoft 365 Apps for Enterprise, Microsoft Office L...](#)
1 vulnerabilities
- 9.6** [Google Chrome, Google Chrome Enterprise, Microsoft Edge \(Chromi...](#)

Tested scan profiles

[Configuration Scan: Windows Workstation](#)



[Vulnerability Scan: Windows \(Professional 2.0\)](#)



Ale nie zapominajmy o patchowaniu ;)

Overview

Risk level



[2338 vulnerabilities found \(therefrom 1083 severe\)](#)

Vulnerabilities found



- High threat
1091 (47%)
- Medium threat
1182 (51%)
- Low threat
65 (3%)

Top 5 vulnerabilities

- 10** [CVE-2009-1571](#)
Mozilla Firefox, Thunderbird and SeaMonkey Use-After-Free HTML P...
CVSS Version: 2.0
3 hours ago
- 10** [CVE-2009-3070](#)
Mozilla Firefox before 3.0.14 allow Denial of Service Vulnerability

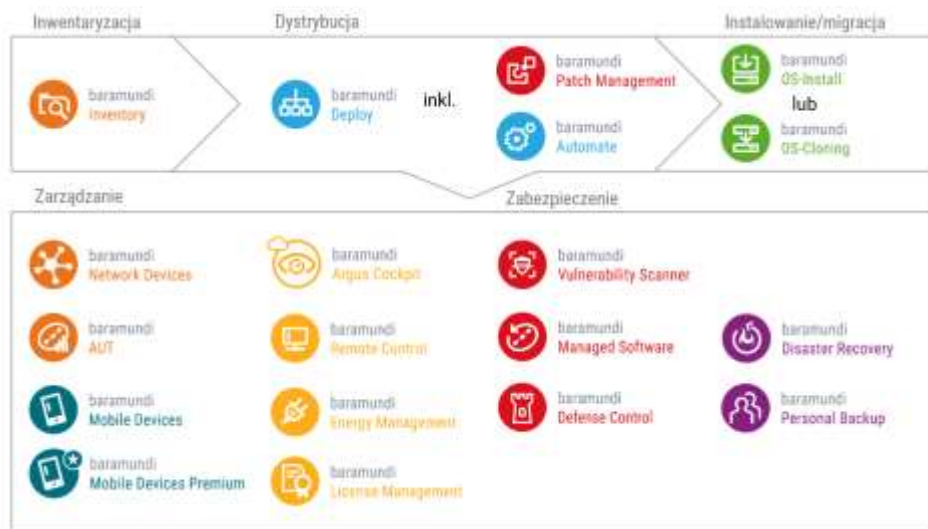
[2338 vulnerabilities found](#)

Top 5 vulnerable products

- 10** [Mozilla Firefox, Mozilla Firefox ESR, Mozilla Thunderbird](#)
488 vulnerabilities
- 10** [Mozilla Firefox](#)
461 vulnerabilities
- 10** [Microsoft Windows, Microsoft Windows Server, Microsoft Windows S...](#)
331 vulnerabilities
- 10** [Mozilla Firefox, Mozilla Firefox ESR](#)

Tested scan profiles






Web: www.baramundi.pl


Empower your IT


**VIII FORUM
KIEROWNIKÓW IT
W ADMINISTRACJI**



VIII FORUM KIEROWNIKÓW IT W ADMINISTRACJI

 **24-26.04.2023**

 ZAKOPANE
BACHLEDA HOTEL KASPROWY

 forum.itwadministracji.pl



Dziękuję za uwagę