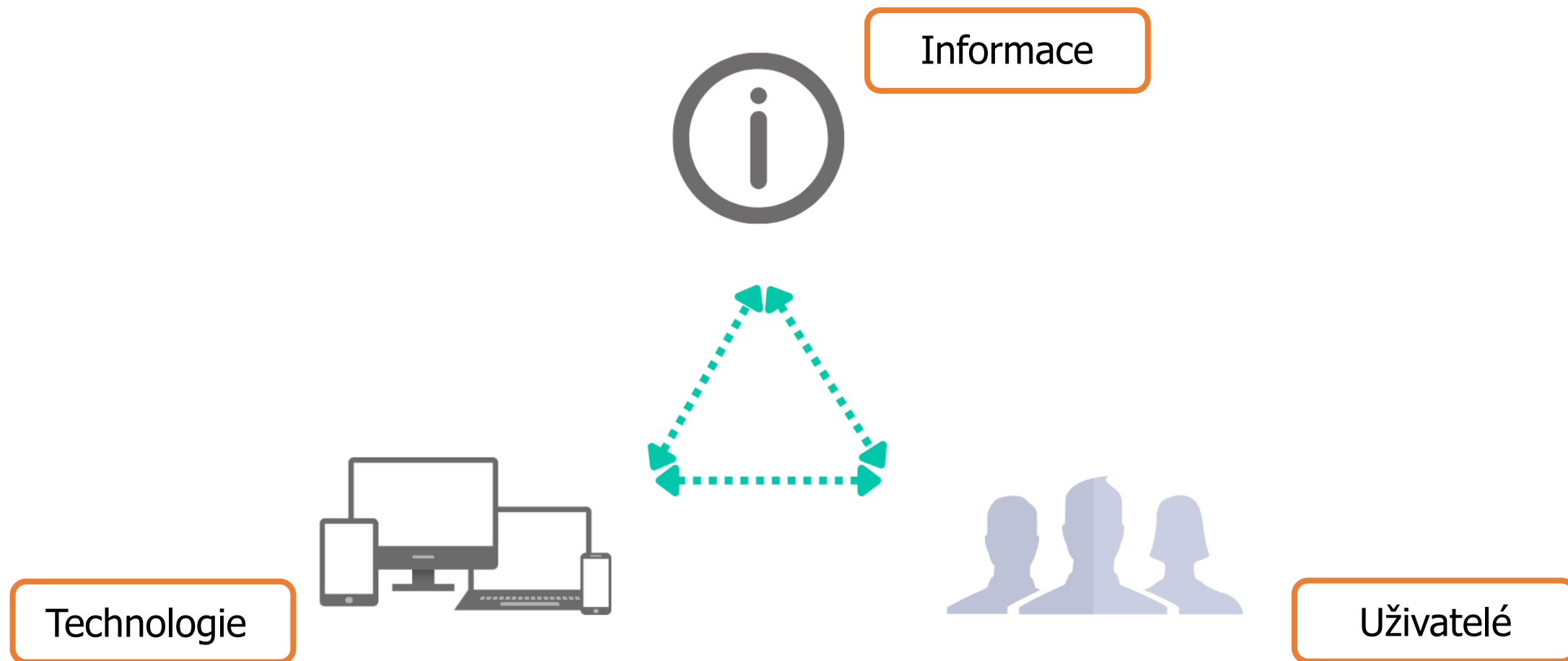




COMGUARD - Ohlédnutí za rokem 2021 optikou služby ThreatGuard a PhishTest

Roman Jiráček, Account & Vendor Manager

Stolička bezpečnosti



PhishTest – simulované phishingové kampaně

[O365-SPAM] Váš balík nebyl doručen.



Česká pošta <notificaciones.sjgp@tsjcdmx.g>

Komu Sales

↩ Odpovědět

↩ Odpovědět všem

→ Přeposlat



po 21.03.2022 6:15

V této zprávě byly zakázány odkazy a jiné funkce. Pokud chcete tyto funkce povolit, přesuňte zprávu do složky Doručená pošta. Tato zpráva byla převedena do formátu prostého textu.

<<https://www.ceskaposta.cz/CeskaPosta-theme/images/cp/logo.png>>

Vážený zákazník,

Všimli jsme si, že vaše objednávka DKRMH60562763, sledovací číslo L938478764, čeká na odeslání kvůli chybějící adrese. Vyplňte svou adresu kliknutím na následující odkaz:

Sledujte svou objednávku <<https://shor.at/U5G9seEQ>>

Stačí vyplnit všechny údaje o vaší poštovní adrese; Balíček bude doručen 48 hodin po zákroku. Další informace vám zůstávají k dispozici.

Převážné náklady: 40,20 CZK

Zákaznický servis Česká pošta

Čení Vašeho konta

022 22:32

[@ekonto.net](#)>

Nové upozornění:

... v ohrožení. Někdo se právě pokusil přihlásit z neznámého zařízení. Byli jste to vy?

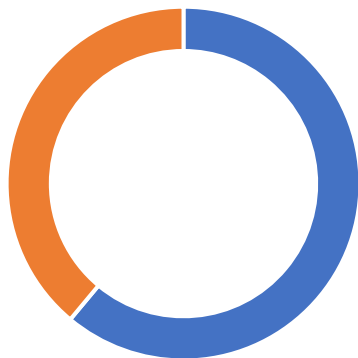
Poloha: Kaliningrad, Ruská Federace

Typ zařízení: iPhone 11

Pokud jste to nebyli vy, pomozte nám zabezpečit Váš účet kliknutím na tlačítko níže

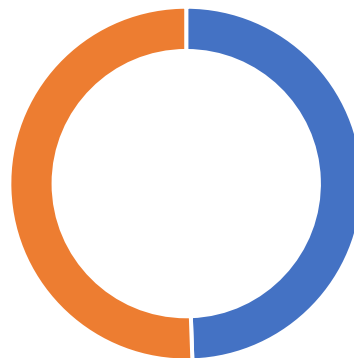
[AUTORIZACE](#)

Otevření emailu 38,94%



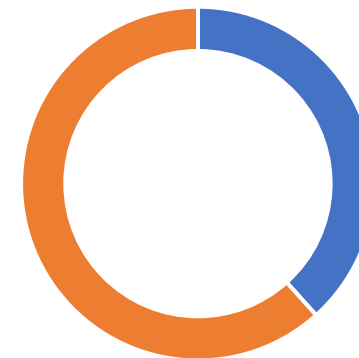
■ Neotevření emailu ■ Otevření emailu

Kliknutí na odkaz 50,55%



■ Nekliknutí na odkaz ■ Kliknutí na odkaz

Zadaná data 61,65%



■ Nezadaná data ■ Zadaná data

PhishTest - ukázka



st 12.05.2021 15:25

Admin Společnosti <admin@serviceict.cz>

Aktivace Vašeho Office365 účtu

Komu Testovaný Pepíček



Vážený uživateli,

Z důvodu migrace na Microsoft Office 365 je nutné provést aktivaci Vašeho Office365 účtu.

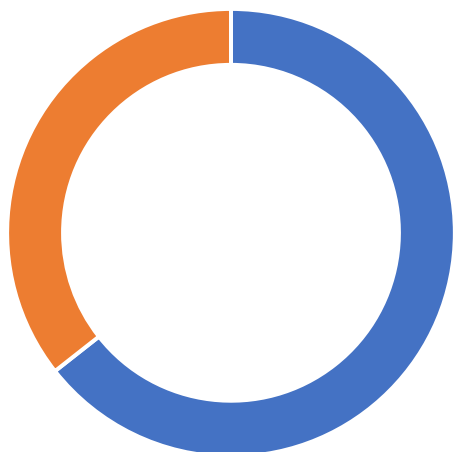
Aktivaci spustíte zadáním uživatelského jména a hesla do Windows na následujícím odkazu: [Vytvoření hesla Office 365 Microsoft Office 365 Team!](#)

Další informace k resetování hesla a ochraně soukromí naleznete na webu Microsoft.com.

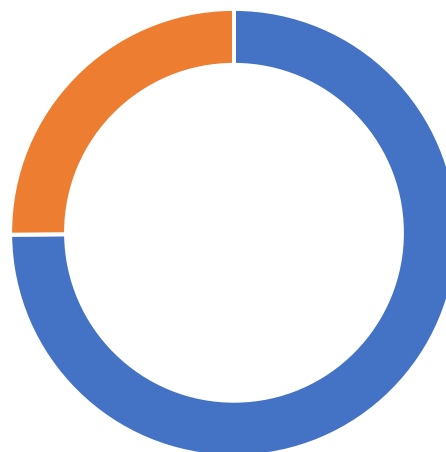
PhishTest – statistiky

- Výsledky phishingových kampaní testování v regionu

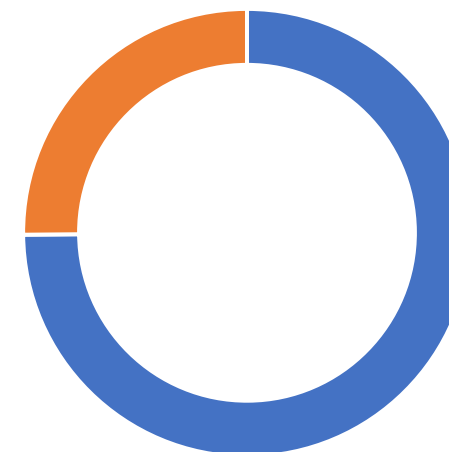
Otevření emailu 35,60%



Kliknutí na odkaz 25,14%



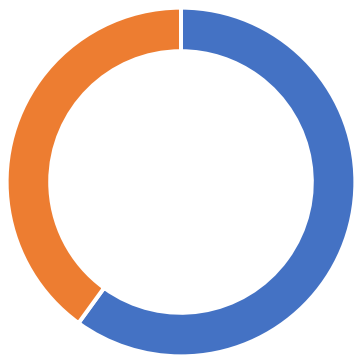
Zadaná data 16,78%



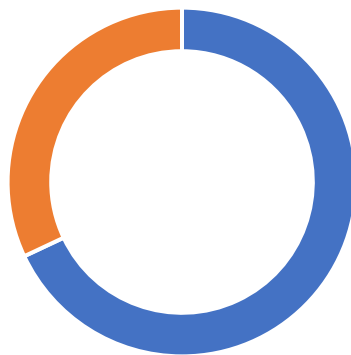
- Zdroj: COMGUARD PhishTest

- Porovnání dvou phishingových kampaní u vybraného klienta

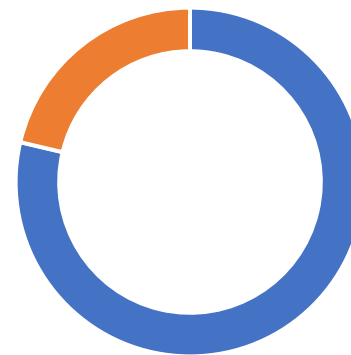
Otevření emailu 40,00%



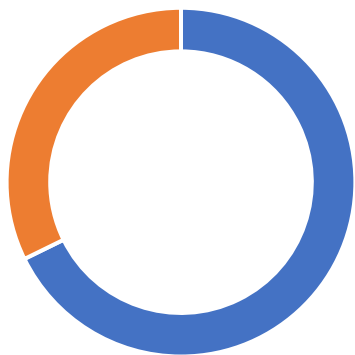
Kliknutí na odkaz 32,00%



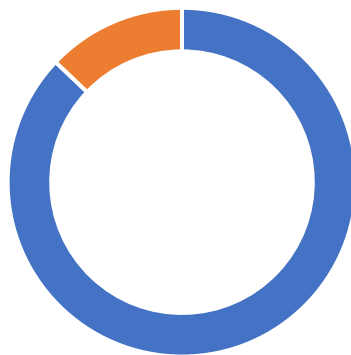
Zadaná data 21,33%



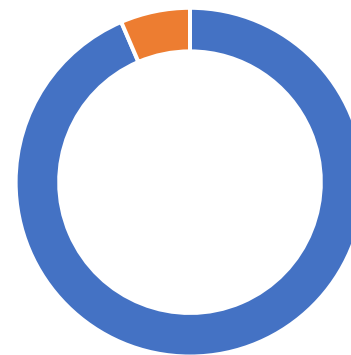
Otevření emailu 32,26%



Kliknutí na odkaz 12,90%



Zadaná data 6,45%



- Zdroj: COMGUARD PhishTest

Jak služba funguje?

- Testování je prováděno pomocí e-mailů, které simulují V
- Vytvoření scénáře útoku - vizuálu podvodného e-mailu a
- Spuštění kampaně rozesláním vybraných podvodných e
- Sledování průběhu kampaně po smluvenou dobu.
- Sběr dat a jejich vyhodnocení.
- Závěrečná zpráva obsahující podrobné zhodnocení kampaně a bezpečnosti.

Běžné služby

Otestování uživatelů pomocí phishingového emailu na běžné služby např. Office365 nesoucí link a odkazující na podvrženou stránku.

Úroveň 1



Custom služby

Otestování uživatelů pomocí phishingového emailu na Vámi definované služby nesoucí link a odkazující na podvrženou stránku.

Úroveň 2



Malware příloha

Otestování uživatelů pomocí phishingového emailu obsahujícího malware přílohu.

Úroveň 3



Na míru

Otestování uživatelů dle Vašich specifických požadavků a přání.

Kontaktujte nás

Úroveň 4



Hlavní přínosy PhishTestu pro Vás

- Posílíte povědomí zaměstnanců o IT bezpečnosti.
- Zvýšíte odolnost zaměstnanců před phishingovými útoky.
- Zavedete další formu ochrany v rámci kybernetické bezpečnosti - prevenci.
- Ošetříte jeden z nejčastějších vektorů útoku.
- Získáte přehled o úrovni odolnosti Vaší společnosti před cílenými útoky.
- Snížíte pravděpodobnost bezpečnostního incidentu.

Kritické hrozby roku 2021:

- Vzdálené převzetí kontroly v Apache Server

 **Microsoft** | **MSRC** | [Security Updates](#) | [Acknowledgements](#) | [Developer](#)

[MSRC](#) > [Customer Guidance](#) > [Security Update Guide](#) > [Vulnerabilities](#) > **CVE 2021 38647**

 We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. [Privacy Statement](#) [Third-Party Cookies](#)

 Welcome to the new and improved Security Update Guide! We'd love your feedback. [Please click here to share your thoughts](#) or email us at msrc_eng_support@microsoft.com. Thank you!

Open Management Infrastructure Remote Code Execution Vulnerability

CVE-2021-38647

On this page ▾

Security Vulnerability

Released: Sep 14, 2021 Last updated: Sep 20, 2021

Assigning CNA:  Microsoft

[CVE-2021-38647](#) 

CVSS:3.0 9.8 / 8.5 

Virtuální bezpečnostní analytik

- Výsledek nepřetržité práce teamu bezpečnostních analytiků
 - Databáze aktuálních hrozeb pro Vaše IT
 - Prověřené návrhy nápravných opatření
- Možnost filtrace hrozeb dle Vašich aktiv
- Dostupné formou webového portálu s notifikacemi
 - Chat s podporou expertního teamu



Stále dostupná, aktuální, strukturovaná databáze hrozeb a opatření

The screenshot displays the ThreatGuard web application interface. At the top, the navigation bar includes the ThreatGuard logo, a home icon, and links for 'Přehled hrozeb', 'CVE', 'Můj ThreatGuard', 'Novinky', 'Analýza souborů', and a user profile for 'Roman Jiráček'. A secondary bar contains an 'Administrace' link.

The main content area is divided into several sections:

- Vítejte Roman Jiráček**: A personalized greeting with the ThreatGuard logo.
- Novinky**: A list of recent news items, including 'TOP 5 hrozeb za BŘEZEN 2022' and 'ThreatGuard 3.0: Nové funkcionality v systému!'. A 'Zobrazit novinky' button is at the bottom.
- Blog**: A list of blog posts, including 'Lovkyně hrozeb' and 'Princip nejnižších oprávnění'. A 'Zobrazit články' button is at the bottom.
- Vybíráme pro Vás**: A section with three cards highlighting specific vulnerabilities:
 - Vzdálené spuštění kódu ve Spring Framework**: Vendor: Cisco, VMware; Severity: High; Type: Vulnerability. Updated 4.4.2022.
 - Kritická chyba v GitLab umožňuje kompromitaci účtů**: Vendor: GitLab Inc.; Severity: High; Type: Vulnerability. Updated 4.4.2022.
 - Dvě zranitelnosti v Rockwell Automation Studio 5000 Logix Designer umožňuje stažení škodlivých programů**: Vendor: Rockwell Automation; Severity: High; Type: Vulnerability. Updated 4.4.2022.

On the right, a smartphone displays the mobile version of the ThreatGuard app, mirroring the desktop layout with the user profile and news sections.

Mitigácia Log4Shell

Základní údaje

ID	1946	Přidáno
Úplnost reportu	plný	Aktualizováno
Typy	Vulnerability	Geolokace
Závažnost	vysoká	Autor

Ověřenost	Opatření třetí strany	Přidáno	13.12.2021 14:58
		Aktualizováno	27.12.2021 14:57
Úplnost reportu	plný		
Vytvořil	Dáša Sedláková		

Přílohy

Zdroje

<https://logging.apache.org/log4j/2.x/security.html>
<https://www.marketscreener.com/quote/stock/RAPID7-INC-23055722/news/Rapid7-Widespread-Exploitation-of-Critical-Remote-Code-Execution-in-Apache-Log4j-37284964/>
<https://www.cisa.gov/uscert/ncas/alerts/aa21-356a>

Náprava

Administrátorom odporúčame čo najskor upgradovať na verziu Log4j 2.15.0, ktorá zraniteľnosť opravuje:

https://logging.apache.org/log4j/2.x/security.html#Fixed_in_Log4j_2.15.0

Aktualizace: CVE-2021-45046

Log4j 1.x není touto zranitelností ovlivněn. Pokud v rámci Log4j2 nevyužíváte defaultní konfiguraci, doporučujeme co nejdříve update na verzi Log4j 2.16.0.

Opatření

Aktualizace

"Log4Shell" (CVE-2021-44228) - LogRhythm

"Log4Shell" (CVE-2021-44228) - Sophos

"Log4Shell" (CVE-2021-44228) - Rapid7

"Log4Shell" (CVE-2021-44228) - Forcepoint SMC

Mitigação Log4Shell

"Log4Shell" (CVE-2021-44228) - McAfee

Popis

Priama oprava

Kritická zraniteľnosť CVE-2021-44228 v Apache Log4j bola opravená vo verzii 2.15. Nadväzujúca menej závažná zraniteľnosť (CVE-2021-45046 s CVSS 3.7) v Apache Log4j bola opravená vo verzii 2.16. A ďalšia závažná zraniteľnosť CVE-2021-45046 je opravená vo verzii 2.17.

Čo najskôr identifikujte, zmiernite a aktualizujte ovplyvnené produkty, ktoré používajú Log4j, na najnovšiu opravenú verziu:

- Pre prostredia používajúce Javu 8 alebo novšiu inovujte na Log4j verziu 2.17.0 (vydaná 17. decembra 2021) alebo novšiu.
- Pre prostredia používajúce Javu 7 inovujte na Log4j verziu 2.12.3 (vydaná 21. decembra 2021). Poznámka: Java 7 je momentálne na konci životnosti a organizácie by mali upgradovať na Javu 8.

Manuálna oprava

Pokiaľ z akéhokolvek dôvodu nemôžete aktualizovať, vo vydaniach novších (alebo rovnakých) ako verzia 2.10 možno zraniteľnosť zmierniť nastavením systémovej vlastnosti `log4j2.formatMsgNoLookups` alebo premennej prostredia `LOG4J_FORMAT_MSG_NO_LOOKUPS` na hodnotu `true`.

Aplikujte preto parameter `-Dlog4j2.formatMsgNoLookups=True` do príkazu JVM na spustenie aplikácie.

Pre vydania novšie(alebo rovnaké) ako verzia 2.7 a staršie(alebo rovnaké) ako 2.14.1, všetky vzory **PatternLayout** môžu byť upravené tak, aby špecifikovali konvertor správ ako `%m{nolookups}` namiesto pôvodného iba `%m`.

Pre vydania novšie(alebo rovnaké) ako verzia 2.0-beta9 a staršie(alebo rovnaké) ako 2.10.0 je zmiernením odstránenie triedy `IndiLookup` z cesty k triede: `zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/IndiLookup.class`.

Ďalšie opatrenia

Navyše, Verzie JDK väčšie ako 6u211, 7u201, 8u191 a 11.0.1 nie sú ovplyvnené vektorom útoku LDAP. `com.sun.jndi.ldap.object.trustURLCodebase` je nastavený na `false`, čo znamená, že JNDI nemôže načítať vzdialenú kódovú základňu pomocou LDAP.

Ďalším odporúčaním je kontrola prichádzajúcich sieťových požiadavok obsahujúcich string "{indi:".

- **Rozhraní pro integraci do dalších systémů** (SIEM, SOC, SOAR, apod.)
- **Rozšířené možnosti filtrování** - fulltextové vyhledávání, Multiselect vyhledávání s možností našeptávání a CPE
- **Rozšíření datových zdrojů hrozeb** - CSIRT ČR a SK
- **HTML notifikace**
- **Zrcadlení celého CVE katalogu do ThreatGuard v AJ** - nová položka v menu
- **Integrace s McAfee ATD** – nahrajete neznámý soubor nebo URL adresu skrze ThreatGuard do McAfee, kde se otestuje a řekne Vám, jestli je v pořádku nebo kritický

CPE string je název software, aplikace a její konkrétní verze ve formátu, který je standardizovaný

- CPE slovník: [NVD - CPE \(nist.gov\)](https://nvd.nist.gov)

Jak CPE string dohromady?

cpe:<verze – 2.3>:<a,o,h – a=aplikace, o=operační system, h=hardware device
>:<vendor>:<produkt>

- Např. cpe:

The screenshot displays the ComGuard web interface. On the left, a sidebar contains a 'CPE' search section with a text input field, a 'Hledat' button, and a 'Uložit filtr' section with a 'Název filtru' input field. The main content area shows a search for the CPE string 'cpe:2.3:o:microsoft:windows_10:1803:*:*:*:*:*'. Below the search results, a threat entry is highlighted: 'Zranitelnost v NTFS sýtémů Windows umožňuje způsobit DOS.' with details: Vendor: Microsoft, Štítky: Windows 10, Závažnost: střední, Typy: DoS, Vulnerability, and a 'DOS' icon. On the right, a 'Přehled hrozeb' (Threat Overview) section is visible, featuring a search bar and a table of filters including 'Vendori', 'Zařízení', 'Úplnost reportu', 'Geolokace', 'CPE', 'Štítky', 'Typy', and 'Závažnost'. The interface includes various buttons like 'Hledat', 'Uložit', 'Resetovat filtr', and 'Seřadit'.

CVE katalog

- Zrcadlení celého CVE katalogu do ThreatGuard v angličtině – nová položka v menu
- **Možnosti filtrování v CVE databázi – aktuálně:**
 - Dle ID u dané CVE
 - Dle CVSS
 - Poslední aktualizace
 - Publikováno

ThreatGuard		
Administrace		
ID	CVSS	Shrnutí
	-	
CVE-2021-44581	5	An SQL Injection vulnerability exists in Kreado Kreasfero 1.5 via the id parameter.
CVE-2022-25521	10	UNNO v03.11.00 was discovered to contain access control issue.
CVE-2021-45865	7.5	A File Upload vulnerability exists in Sourcecodester Student Attendance Manageent System 1.0 via the file upload function.
CVE-2022-1032	6.5	Insecure deserialization of not validated module file in GitHub repository crater-invoice/crater prior to 6.0.6.
CVE-2022-27441		A stored cross-site scripting (XSS) vulnerability in TPCMS v3.2 allows attackers to execute arbitrary web scripts or HTML via

CVE-2021-45865

ID

CVE-2021-45865

Shrnutí

A File Upload vulnerability exists in Sourcecodester Student Attendance Manageent System 1.0 via the file upload functionality.

▼

Reference

<https://github.com/lohyt/Code-execution-via-vulnerable-file-upload-functionality-found-in-Student-Attendance-Management-System>

▼

Zranitelné konfigurace

cpe:2.3:a:student_attendance_management_system_project:student_attendance_management_system:1.0:*:*:*:*:*

▼

CVSS

7.5

CWE

CWE-434

Přístupnost

Authentication	Complexity	Vector
NONE	LOW	NETWORK

Dopad

Availability	Confidentiality	Integrity
PARTIAL	PARTIAL	PARTIAL

CVSS vektor

AV:N/AC:L/Au:N/C:P/I:P/A:P

Poslední velká aktualizace

4.4.2022 - 21:29

Publikováno

29.3.2022 - 01:15

Poslední úpravy

4.4.2022 - 21:29

Integrace s McAfee Advanced Threat Defense

McAfee

Threat Analysis Report

URL

hxxps://www.seznam.cz/

Malware Name

Analysis.Dynamic

URL Submitted

2022-03-11 09:06:00 UTC

File Size

22 -

Show More

Hash Values

File Details

MD5 Hash Identifier

D0D3D6C3B870C6ABFC0594DDA539C

Screenshots

2

Hide hash values

File Type

application/url

Hide file details

Microsoft Windows 7 Professional Service Pack 1 (build 7601, version 6.0.6002.18147)

Windows® Internet Explorer version: 8.0.7601.17514

Microsoft Office version: 2010

PDF Reader version: DC

No Flash player installed

Flash player plugin version: 32.0.0.387

Platform Version 4.14.0.7

Detection Package Version 4.14.0.220107

Hide environment

Baltaxe activated but not infected

Name

Reason

hxxps://www.seznam.cz/

loaded by MATD Analyzer

Timeline Activity

Processes

Files

Registry Operations

Network Operations

Multiple

hxxps://www.seznam.cz/

Select Any Area to Zoom In

0 3 6 9 12 15 18

Offset In s

Jump to Timeline Details

Techniques/SubTechniques Observed (MITRE ATT&CK™ Matrix)

Technique

System Services

Service Execution

Adversaries may abuse the Windows service control manager to execute malicious commands or payloads. The Windows service control manager (services.exe) is an interface to manage and manipulate services. The service control manager is accessible to users via GUI components as well as system utilities such as sc.exe and [Net].

Attempted to execute service

2 - Low

Hide Artifacts

Hidden Files and Directories

Adversaries may set files and directories to be hidden to evade detection mechanisms. To prevent normal users from accidentally changing special files on a system, most operating systems have the concept of a hidden file. These files don't show up when a user browses the file system with a GUI or when using normal commands on the command line. Users must explicitly ask to show the hidden files either via a series of Graphical User Interface (GUI) prompts or with command line switches (dir /a for Windows and ls -la for Linux and macOS).

Hid content by modifying its attributes

2 - Low

System Network Configuration Discovery

Adversaries may look for details about the network configuration and settings of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information.

Queried for system network configuration information

2 - Low

Screenshots

Note: a pop-up window was detected during dynamic analysis so user interaction may be required in order to fully analyze this sample

Images: 2

3e8fa.jpg

Aplikace Internet Explorer nemůže zobrazit tuto webovou stránku. - Windows Internet Explorer

https://www.seznam.cz/

Bing

Oblíbené položky

Navrhované weby

Aplikace Internet Explorer nemůže zobrazit tuto w...

Stránka

Zabezpečení

Nástroje

Aplikace Internet Explorer nemůže zobrazit tuto webovou stránku.

Můžete vyzkoušet následující možnosti:

Diagnostika potíží s připojením

Další informace

Hotovo

Internet | Chráněný režim: Vypnuto

100%

36bcb.jpg

Detail

Detail

Detail

Hlavní přínosy ThreatGuard pro Vás

- Rychlý přehled o nejnovějších hrozbách pro vaše IT
- Přehlednou aktuální databázi hrozeb včetně návrhů nápravných opatření
- Pouze informace, které potřebujete - filtrace IT hrozeb dle vašich preferencí a potřeb
- Detailní filtrování na úrovni verze operačního systému nebo aplikace
- Emailová notifikace pro vaši pružnou reakci
- Dostupnost na všech rozšířených platformách Windows, Android, iOS
- Online chat s podporou IT expertů



Děkuji za pozornost!