

1. Co je to vlastně ThreatGuard? Proč ho potřebuji?
2. Na co potřebuji ThreatGuard, když mám skener zranitelností?
3. Pod pojmem hrozby v portálu ThreatGuard popisujete i zranitelnosti, které mohu odhalit za použití skeneru zranitelností, je to tak?
4. Lze službu ThreatGuard PORTAL používat i v anglickém jazyce?
5. Je možné službu ThreatGuard provázat na řešení SIEM nebo Trellix ePO?
6. Jaká jsou kritéria pro výběr sledovaných hrozeb?
7. Proč např. zranitelnost NetBackup CVE-2017-885[6-9] není v ThreatGuard uvedena?
8. S jakým zpožděním se objeví nová hrozba ve službě ThreatGuard?
9. Lze službu ThreatGuard přizpůsobit konkrétním požadavkům, tedy budu sledovat pouze technologie, které mám v infrastruktuře nasazené?
10. Jak funguje real-time chat/support a co zákazníkovi přinese v rámci licence ThreatGuard HelpDesk?
11. Testujete nápravy a opatření k jednotlivým hrozbám uvedeným v ThreatGuard před jejich zveřejněním na portálu?
12. Zabýváte se pouze technologiemi z vašeho portfolia nebo uvádíte do ThreatGuard i hrozby týkající se jiných výrobců?

1. Co je to vlastně ThreatGuard? Proč ho potřebuji?

ThreatGuard je Cyber Threat Intelligence, která za Vás vyhodnocuje relevantní kybernetické hrozby až z několika desítek zdrojů. Hrozby roztřídí dle priority, určí vektory šíření a připraví pro Vás nápravná opatření. Zákazníci využívající produkty Trellix také jistě ocení zasílání hotových konfiguračních souborů, jejichž importem do ePO se automaticky upraví nastavení a politiky. Za měsíční poplatek získáte **tým stálých zaměstnanců – bezpečnostních specialistů**, kteří průběžně vybírají a zveřejňují z velkého množství upozornění jen ty relevantní a aktuální hrozby na webovém portálu.

Po přihlášení uvidíte všechny aktuální IT hrozby a případně (volitelné) jste na nově evidované hrozby upozorňováni emailem, a to pouze v případě, že nějaká nově evidovaná hrozba vyplývá z Vašeho aktivního filtru, který si v ThreatGuard můžete nastavit. Služba ThreatGuard se liší od konkurence mimo jiné **přesně stanoveným procesem posuzování hrozeb**. Důležitá je rychlost, protože od renomovaných bezpečnostních firem jsou informace bohužel často týdny až měsíce zastaralé.

2. Na co potřebuji ThreatGuard, když mám skener zranitelností?

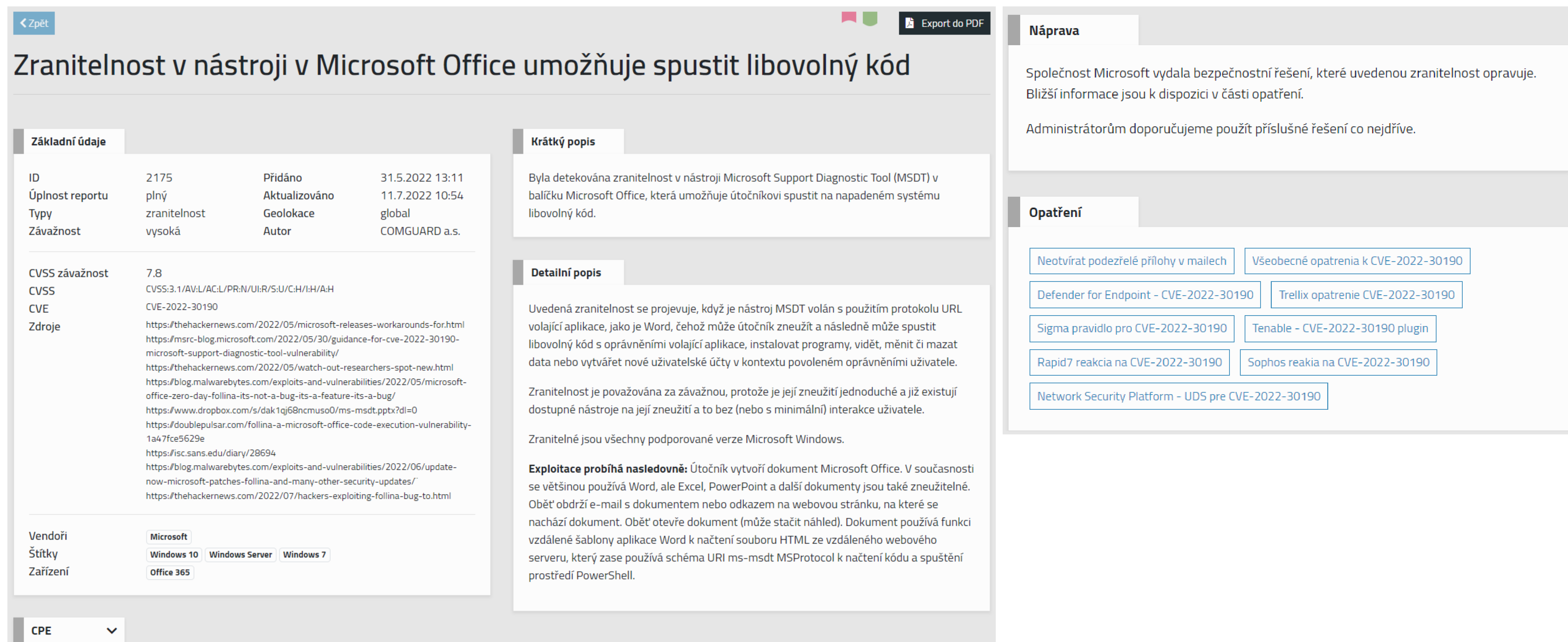
ThreatGuard a skener zranitelností jsou dva naprosto odlišné světy.

Skener zranitelností primárně testuje Vaši vnitřní síť a kontroluje, zda byly aplikovány patche na známé zranitelnosti a zda jsou všechny OS a firmware aktuální.

ThreatGuard hlídá bezpečnostní hrozby – zranitelnosti jsou podmnožinou jeho zaměření. O **hrozbě skener zranitelností nemůže vědět a nemůže v mnoha případech pomoci**. Reakce na hrozbu není jen patchování, ale soubor komplexních opatření od personálních např. neotevírat e-mail, až po nastavení konkrétních zařízení – takovou možnost skener nemá.

3. Pod pojmem hrozby v portálu ThreatGuard popisujete i zranitelnosti, které mohou odhalit za použití skeneru zranitelností, je to tak?

Ano, některé zranitelnosti lze síťovým skenerem odhalit, je jich však zlomek ve srovnání se všemi hrozbami. Pro vaši představu předkládáme jednu z mnoha hrozeb z našeho portálu, kterou skener zranitelností nemá šanci zachytit.



Zranitelnost v nástroji v Microsoft Office umožňuje spustit libovolný kód

Základní údaje

ID	2175	Přidáno	31.5.2022 13:11
Úplnost reportu	plný	Aktualizováno	11.7.2022 10:54
Typy	zranitelnost	Geolokace	global
Závažnost	vysoká	Autor	COMGUARD a.s.

CVSS závažnost 7.8
CVSS CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVE CVE-2022-30190
Zdroje <https://thehackernews.com/2022/05/microsoft-releases-workarounds-for.html>
<https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/>
<https://thehackernews.com/2022/05/watch-out-researchers-spot-new.html>
<https://blog.malwarebytes.com/exploits-and-vulnerabilities/2022/05/microsoft-office-zero-day-follina-its-not-a-bug-its-a-feature-its-a-bug/>
<https://www.dropbox.com/s/dak1qj6nmsuo0/ms-msdt.pptx?dl=0>
<https://doublepulsar.com/follina-a-microsoft-office-code-execution-vulnerability-1a47fce5629e>
<https://isc.sans.edu/diary/28694>
<https://blog.malwarebytes.com/exploits-and-vulnerabilities/2022/06/update-now-microsoft-patches-follina-and-many-other-security-updates/>
<https://thehackernews.com/2022/07/hackers-exploiting-follina-bug-to.html>

Krátký popis

Byla detekována zranitelnost v nástroji Microsoft Support Diagnostic Tool (MSDT) v balíčku Microsoft Office, která umožňuje útočnickovi spustit na napadeném systému libovolný kód.

Detailní popis

Uvedená zranitelnost se projevuje, když je nástroj MSDT volán s použitím protokolu URL volající aplikace, jako je Word, čehož může útočník zneužít a následně může spustit libovolný kód s oprávněními volající aplikace, instalovat programy, vidět, měnit či mazat data nebo vytvářet nové uživatelské účty v kontextu povoleném oprávněními uživatele.

Zranitelnost je považována za závažnou, protože je její zneužití jednoduché a již existují dostupné nástroje na její zneužití a to bez (nebo s minimální) interakcí uživatele.

Zranitelné jsou všechny podporované verze Microsoft Windows.

Exploitační průběh následovně: Útočník vytvoří dokument Microsoft Office. V současnosti se většinou používá Word, ale Excel, PowerPoint a další dokumenty jsou také zneužitelné. Oběť obdrží e-mail s dokumentem nebo odkazem na webovou stránku, na které se nachází dokument. Oběť otevře dokument (může stačit náhled). Dokument používá funkci vzdálené šablony aplikace Word k načtení souboru HTML ze vzdáleného webového serveru, který zase používá schéma URI ms-msdt MSProtocol k načtení kódu a spuštění prostředí PowerShell.

Náprava

Společnost Microsoft vydala bezpečnostní řešení, které uvedenou zranitelnost opravuje. Bližší informace jsou k dispozici v části opatření.

Administrátorům doporučujeme použít příslušné řešení co nejdříve.

Opatření

- Neotvírat podezřelé přílohy v mailch
- Všeobecná opatření k CVE-2022-30190
- Defender for Endpoint - CVE-2022-30190
- Trellix opatření CVE-2022-30190
- Sigma pravidlo pro CVE-2022-30190
- Tenable - CVE-2022-30190 plugin
- Rapid7 reakce na CVE-2022-30190
- Sophos reakce na CVE-2022-30190
- Network Security Platform - UDS pro CVE-2022-30190

4. Lze službu ThreatGuard PORTAL používat i v anglickém jazyce?

Ano, portál je dostupný, jak v českém, tak i v anglickém jazyce.

5. Je možné službu ThreatGuard provázat na řešení SIEM nebo Trellix ePO?

Služba ThreatGuard PORTAL nabízí opatření proti vybraným hrozbám formou exportu politik pro ePO v ceně služby. Forma předpřipravených konfiguračních exportů pro nastavení doporučených úprav v ePO je velmi efektivní způsob, jak aplikovat doporučení a zkušenosti analytiků ThreatGuard ve vlastní síti. **Provázání služby ThreatGuard a řešení SIEM je možné od verze ThreatGuard 3.0.**

Případně kontaktujte obchodního zástupce s popisem vašich požadavků na integraci, služba je stále vyvíjena a zlepšována.

6. Jaká jsou kritéria pro výběr sledovaných hrozeb?

Kritéria jsou interně v týmu analytiků stanovena následovně:

Musí se jednat o hrozbu, která je v danou chvíli reálná a ne pouze teoretická

- Existence zranitelnosti, pro kterou není známá forma aplikovatelného zneužití, nepovažujeme za podstatnou a zranitelnost do ThreatGuard nezařadíme. **Šetříme tak Váš čas pouze pro podstatné a relevantní hrozby.**

- Zveřejnění exploitu nebo zdokumentované pokusy o zneužití určité zranitelnosti je pro nás signál, že je nutné hrozbu do ThreatGuard zařadit.

Hrozba se musí týkat našeho regionu

- Jakákoliv globální hrozba nebo lokální malwarová/phishingová kampaň je relevantní.

- Phishingová/malwarová kampaň mířící velmi specificky na region mimo CZ/SK je pro ThreatGuard irelevantní.

Hrozba se musí týkat aktiv, která jsou relevantní pro firemní použití

- Nezabýváme se např. zranitelnostmi domácích routerů, soukromých blogovacích platform, herních systémů, apod.

- Velmi vážně bereme hrozby týkající se aplikačních serverů, Active Directory, Linuxových serverů, aktivních prvků apod. Ze všech zpracovávaných zdrojů projde našimi filtry cca 10% všech možných zpráv, upozornění, novinek, apod., takže odfiltrujeme zbytečný šum irelevantní pro ochranu infrastruktury.

7. Proč např. zranitelnost NetBackup CVE-2017-885[6-9] není v ThreatGuard uvedena?

Důvodem je, že pro zmíněné zranitelnosti neexistuje zatím (v čase psaní odpovědi) veřejně dostupný exploit ani zmínka o tom, že by zranitelnost byla zneužívána některými útočníky nebo malwarem.

8. S jakým zpožděním se objeví nová hrozba ve službě ThreatGuard?

Jedná se o best-effort aktivitu. Vyhodnocování probíhá v pracovní dny v čase 8:00–17:00 a proces je nastaven tak, aby informace o existenci hrozby byly zveřejněny co nejrychleji po ověření podmínek uvedených výše. Analytik hrozbu zveřejňuje samostatně, abychom eliminovali zpoždění způsobené zavedením schvalovacího procesu. Hrozby jsou kontrolovány zpětně dalším členem týmu, který případně může navrhnout jejich stažení nebo přepracování.

9. Lze službu ThreatGuard přizpůsobit konkrétním požadavkům, tedy budu sledovat pouze technologie, které mám v infrastruktuře nasazené?

Aktivní filtry – filtrace je možná již dnes na základě dostupných aktiv.

10. Jak funguje real-time chat/support a co zákazníkovi přinese v rámci licence ThreatGuard HelpDesk?

V případě zakoupení licence ThreatGuard HelpDesk máte k dispozici real-time chat, kdy budete moci v reálném čase řešit své specifické požadavky a dotazy na hrozby s týmem odborníků, který za celou službou stojí.

11. Testujete nápravy a opatření k jednotlivým hrozbám uvedeným v ThreatGuard před jejich zveřejněním na portálu?

Ano, všechny nápravy a opatření k jednotlivým hrozbám jsou napřed otestovány v rámci našeho labu a až poté, co 100% ověříme jejich funkčnost, tyto ochranné prvky zveřejníme na portále ThreatGuard.

12. Zabýváte se pouze technologiemi z vašeho portfolia nebo uvádíte do ThreatGuard i hrozby týkající se jiných výrobců?

Chápeme, že abychom byli s touto službou úspěšní, musíme se zajímat i o technologie výrobců, které v ČR a SR nezastupujeme. Proto v ThreatGuard naleznete i technologie jiných výrobců (Fortinet, Cisco, Symantec apod.). Jen takto jsme schopni efektivně pokrýt různorodé IT infrastruktury našich zákazníků informacemi o aktuálních hrozbách.