

# ThreatGuard



## Virtuální bezpečnostní analytik

- ∞ Nevíte, jak čelit nejaktuálnějším bezpečnostním hrozbám?
- ∞ Nalezení příčin a opatření trvá příliš dlouho a malware se šíří dál a způsobuje další škody?
- ∞ Chybí vám dostupnost preventivních opatření na hrozby zaznamenané v ČR a SR?
- ∞ Dokážete určit míru rizika jednotlivých hrozeb pro Vaši společnost?
- ∞ Máte problém určit prioritu nápravným opatřením?

### Potřebné informace na jednom místě

Služba ThreatGuard za vás sleduje aktuální vývoj IT hrozeb v prostředí CZ/SK – EU – svět, relevantní hrozby ohodnotí mírou rizikovosti a hlavně pro vás připraví nápravná opatření, které je vhodné aplikovat. Velkou výhodou služby ThreatGuard je, že na jednom místě máte přehled všech relevantních hrozeb rozdělených dle zařízení, na které cílí, dále dle rizikovosti a podrobného popisu, jakým způsobem se projevuje. Obsah portálu si můžete vyfiltrovat např. podle vámi využívaných zařízení a získáváte tak jen relevantní informace. Službu ThreatGuard PORTAL lze využívat i v anglickém jazyce.

### Unikátní přístup

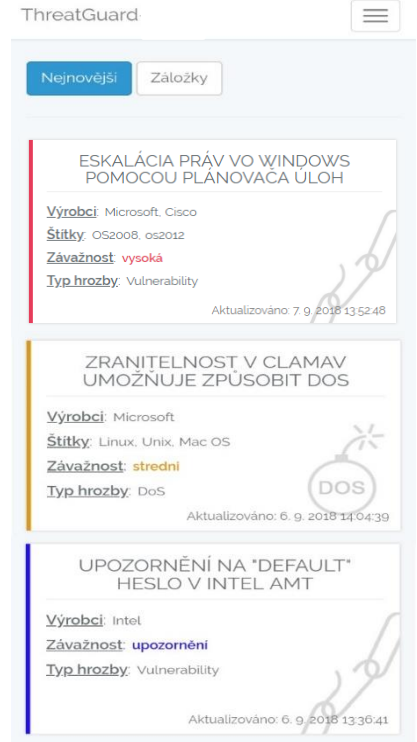
Obsah připravují vybraní specialisté dodavatele na základě vlastních zkušeností, veřejně dostupných informací a simulací. Obsah je uživatelům publikován ve formě ucelených reportů, které mohou být postupně upravovány a obměňovány. Obsah je připravován tak, aby byl srozumitelný bezpečnostním manažerům i správčům konkrétních aktiv a aby mohl sloužit jako podklad pro kvalifikované rozhodnutí, zda je nutné a vhodné hrozbu řešit. Pokud se manažer rozhodne hrozbu řešit, má v reportu rovnou k dispozici informace pro administrátory, kterým informace poskytne jako přímočarý návod pro mitigaci hrozby.

### Možnosti ThreatGuard

**TG Portal** – tým expertů pro vás denně sumarizuje aktuální hrozby a zranitelnosti z více než 30 ověřených zdrojů a vyhodnotí jejich relevantnost pro prostředí organizací v ČR/SR. Vše je srozumitelně popsáno, opatřeno doporučeními na úrovni konfigurací nebo workaroundů. Pomůžeme vám jak s preventivními opatřeními, tak v případě napadení výrazně urychlíme vaši akceschopnost.

**ThreatGuard HelpDesk** – nástavba nad TG Portal přináší navíc možnost zadat vlastní problém, tým expertů zanalyzuje prioritně příčinu a vyhodnotí návrhy opatření, které budou publikovány v rámci Portálu. V ceně TG HelpDesk získá zákazník navíc dostupnost individuálních konzultací a podpory, analýzy příčin a zdrojů prostřednictvím realtime supportu. A to vše i v rámci realizace opatření typických pro prostředí zákazníka.

~ 300.. partnerů/resellerů  
 ~ 3.000.. spokojených klientů  
 ~ 300.000..... zachráněných dat



#### Hlavní přínosy ThreatGuard

- ∞ Pouze relevantní hrozby stručně a přehledně
- ∞ Filtrování dle aktiv, která mě zajímají
- ∞ Omezení šíření hrozby v síti díky okamžitému přístupu do portálu
- ∞ Snadná akceschopná opatření
- ∞ Možnost vložit požadavek na rozpracování konkrétní hrozby
- ∞ Ideální nástroj pro Security Managera
- ∞ Nutný nástroj pro Operation Managera (provozu)
- ∞ Hrozby rozděleny na kategorie: zranitelnost, malware, phishing, ransomware

#### Co přináší ThreatGuard 2.0

- ∞ Webová aplikace postavená přímo na míru požadavkům zákazníků
- ∞ Jednoduchý a přehledný systém (USER friendly)
- ∞ Realtime support expertního týmu
- ∞ Live chat = okamžitá odezva
- ∞ Individuální přístup k řešení vašich požadavků včetně doporučení
- ∞ Emailová notifikace na aktuální hrozby
- ∞ Službu dostupnou v ČR a AJ

ThreatGuard Hrozby Aktivní filtry

Nejnovější Záložky

**ZRANITELNOST V CLAMAV UMOŽŇUJE ZPŮSOBIT DOS**

Výrobci: Microsoft  
 Štítky: Linux, Unix, Mac OS  
 Závažnost: **střední**  
 Typ hrozby: DoS

Aktualizováno: 6. 9. 2018 14:04:39

**V NOVÝCH TELEFONECH SE SYSTÉMEM ANDROID BYL NALEZEN PŘEDINSTALOVANÝ MALWARE**

Výrobci: Řáholec  
 Štítky: Android  
 Závažnost: **vysoká**  
 Typ hrozby: Malware

Aktualizováno: 7. 9. 2018 13:52:01

**UPOZORNĚNÍ NA "DEFAULT" HESLO V INTEL AMT**

Výrobci: Intel  
 Závažnost: **upozornění**  
 Typ hrozby: Vulnerability

Aktualizováno: 6. 9. 2018 13:36:41

← Zpět

**ESKALÁCIA PRÁV VO WINDOWS POMOCOU PLÁNOVAČA ÚLOH**

**Základní údaje**

Úplnost reportu: **plný**  
 Stav reportu: **zpracovaný**  
 Typ: **Vulnerability**  
 Závažnost: **vysoká**  
 Geolokace: Global  
 Přidáno: 06. 09. 2018 14:23  
 Aktualizováno: 06. 09. 2018 14:44

Vytvořil: ThreatGuard

**Náprava**

**Opatření**

Omezení přístupu do C:\Windows\Tasks

**Rozsah působnosti**

Výrobci: Microsoft, Cisco  
 Štítky: OS2008, OS2012  
 Zařízení: Server, Windows PC

**Obsah**

Krátký popis: Chyba v plánovači úloh systému Windows obsahuje chybu, která umožňuje eskalování práv. Chyba zatím není opravena, ale existuje workaroud.

CVSS závažnost: 7.3  
 CVSS link: <https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AVL/ACL/PRL/UIR/SU/CH/HAH>  
 CVE link: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8412>  
 Zdroje: <https://www.kb.cert.org/vuls/id/906424>

**Detailní popis**

Plánovač úloh Microsoft Windows obsahuje chybu v API při zpracování ALPC (Advanced Local Procedure Call), která umožňuje autentifikovanému uživateli přepsat obsah souboru, který by měl být chráněn systémovými ACL. To může být útočným využitím k získání systémových práv.

**ESKALÁCIA PRÁV VO WINDOWS POMOCOU PLÁNOVAČA ÚLOH**

Výrobci: Microsoft, Cisco  
 Štítky: OS2008, OS2012  
 Závažnost: **vysoká**  
 Typ hrozby: Vulnerability

Aktualizováno: 7. 9. 2018 13:52:48

**Popis**

**Opatření třetí strany:**

Úprava ACL k složce C:\Windows\Task

Tato změna není oficiálně podporovaná společností Microsoft. Po změně ACL fungují plánovače úloh a uživatelé mezi v jiném roze. Přeznamí však fungovat úlohy vytvořené legálními nástroji plánovače úloh.

V příkazovém řádku s novějšími právy spusíte následovně příkazy:

```
icacls c:\windows\tasks /remove:g "Authenticated Users" /c
icacls c:\windows\tasks /deny system/OCIOW/D/WDACI
```

Změny ACL vrátíte do původního stavu následujícími příkazy:

```
icacls c:\windows\tasks /remove:d system
icacls c:\windows\tasks /grant:n "Authenticated Users" /R/W/D
```

**Opatření McAfee Endpoint Security - Idea (v testování)**

Access Protection politika

- ALPC\_privilege\_escalation.xml

Politika zakazuje všem uživatelům mimo Local\System vytvářet a modifikovat soubory v umístění C:\Windows\Tasks. Politika je pouze v logovacím režimu, pro blokad je nutné přepsat Action na Block.

Threat Prevention - Exploit Protection signatura

Signatura zabraňuje jakýkoliv přístup všech uživatelů a vytvoření nebo modifikaci souborů v umístění C:\Windows\Task.

```
Rule 1
Process 1
Include OBJECT_NAME 1
-v "*"
}
Target 1
Match FILE 1
Include OBJECT_NAME 1
-v "C:\Windows\Tasks\*"
}
Include -access "CREATE WRITE"
}
```

**Omezení přístupu do C:\Windows\Tasks**

**Základní údaje**

Ověřeno: **testováno**  
 Přidáno: 06. 09. 2018 14:31  
 Neposledy upraveno: 06. 09. 2018 14:31

Přidat: ThreatGuard

**Přiložky**

- Přiložka 1

**Zdroje**

<https://www.kb.cert.org/vuls/id/906424>

**Klientské zobrazení ThreatGuard 2.0**

Platforma ThreatGuard 2.0 nabízí uživatelům nejen detailní přehled o jednotlivých hrozbách, ale také možnost efektivně na tyto hrozby reagovat. Prostřednictvím odborných náprav a opatření vytvořených odborným týmem ThreatGuard.

Garant projektu:

Technologický partner:

