

Co je ThreatGuard?

- **Webový portál** s databází seříděných reálných hrozeb
- Obsahuje **aktivní filtry** a **notifikuje hrozby** emailem
- **Tým IT expertů**, který analyzuje kybernetické hrozby
- **Navrhuje konkrétní a účinná nápravná opatření**

☐ Microsoft
☐ Apple
☐ Cisco
☐ VMware
☐ McAfee
☐ Sophos
☐ Juniper Networks
☐ Hewlett-Packard
☐ Oracle
☐ F5 Networks
☐ Palo Alto Networks

UMOZNUJÍ RCE V
VERZI WINDO

Výrobci: Microsoft

Závažnost: vysoká

Typ hrozby: Vulnerability

Aktualizováno

Zranitelnost

Komponentu v

WIN32K

Výrobci: Microsoft

Závažnost: vysoká

RADAR IT HROZEB

Tým expertů s více jak 10 letou praxí vyhledává reálné IT hrozby a zranitelnosti z ověřených zdrojů a sbírá informace od světových bezpečnostních výrobců a vydává **návrhy nápravných opatření** pro každou hrozbu. **Analyzuje a klasifikuje hrozby podle stupně závažnosti.**

ThreatGuard obsahuje **ucelené reporty** a je připravován tak, aby byl srozumitelný IT odborníkům, bezpečnostním manažerům a slouží jako **podklad pro rychlá a kvalifikovaná rozhodnutí.**

Uživatel má v reportu k dispozici také návrhy **nápravných opatření**, které může rovnou přeposlat kompetentním osobám **jako přímočarý návod k eliminaci hrozby.**

ESKALACE PRIVILEGIÍ VE VMWARE
FUSION, REMOTE CONSOLE A
HORIZON CLIENT PRO MAC

Výrobci: VMware

Závažnost: vysoká

Typ hrozby: Vulnerability

Aktualizováno: 20.3.2020 11:46

**Žádná implementace,
webový portál vás
emailem notifikuje
o kritických hrozbách**

**ŠETŘETE
ČAS A PENÍZE**

ThreatGuard vám šetří čas, peníze a personální zatížení

ThreatGuard analyzuje hrozby za vás a vy tak můžete věnovat čas jiným úkolům. IT hrozby již nechte na nás.

Cisco Firepower Management Center Zranitelnost

Základní údaje

ID	911	Přidáno	18. 10. 2019 12:30
Úplnost reportu:	plný	Aktualizováno	18. 10. 2019 12:30
Typ:	Vulnerability	Geolokace:	Global
Závažnost:	střední		

CVSS závažnost: 5.4
CVSS link: [CVSS 3.0/AVN/ACL/PRL/UIR/SC/CL/IL/AN](#)
CVE link: [CVE-2019-15270](#)
[CVE-2019-15280](#)
[CVE-2019-15268](#)
[CVE-2019-15269](#)

Zdroje: <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-fwprw-stored-xss>
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-fwprw-xss>
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-fwprw-xss>

Výrobci:
Zařízení:

Náprava

Cisco vydalo bezpečnostní protokol
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-fwprw-stored-xss>
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-fwprw-xss>
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-fwprw-xss>

Cisco doporučuje uživatelům updatovat

Opatření

Krátký popis

V Cisco Firepower Management Center

Detailní popis

Reference

AirBank: „Díky ThreatGuard má náš bezpečnostní tým přesnější informace o relevantních hrozbách a je na ně schopen efektivněji reagovat. V důsledku se nám také uvolnily kapacity pro další aktivity v oblasti IT bezpečnosti.“

Meopta: „Osobně jsem neměl moc velké očekávání, nicméně mě služba příjemně překvapila. Hlavně, když jsem přišel na to, jak fungují filtry. Po jejich nastavení se přidaná hodnota služby posunula ještě dál.“



Co získáte díky ThreatGuard?

- Přehled kritických zranitelností a hrozeb pro Vaše technologie
- Obdržíte **setříděné informace** z ověřených informačních zdrojů
- **Kvalifikovaná doporučení** o účinných bezpečnostních opatřeních
- **Návody na ověřenou a vyzkoušenou obranu** při napadení
- **Stanovení míry rizika hrozby** pro vaše konkrétní IT prostředí
- Přístup k **návodům pro nápravná a preventivní opatření**

