COMGUARD

cyber security masters

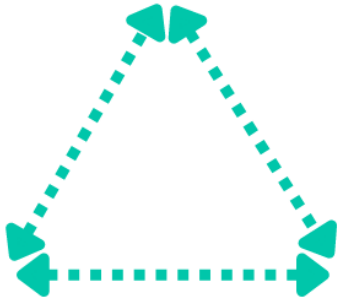
ThreatGuard a PhishTest

Ohlédnutí za rokem 2022 optikou těchto služeb

Roman Jiráček | Senior Account & Vendor Manager

18.09.2023

Informace



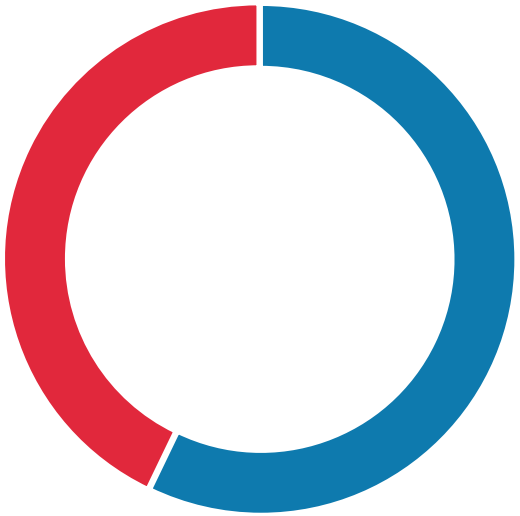
Technologie

Uživatelé

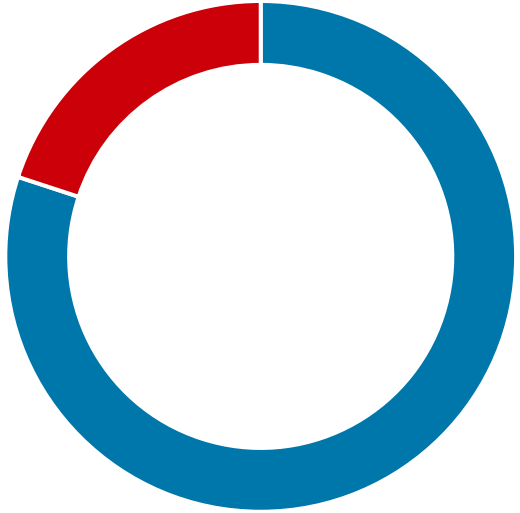
PhishTest – statistiky 2022

- Výsledky phishingových kampaní testování v regionu (Česko a Slovensko)
  - Celkově odesláno **19 tis. emailů**

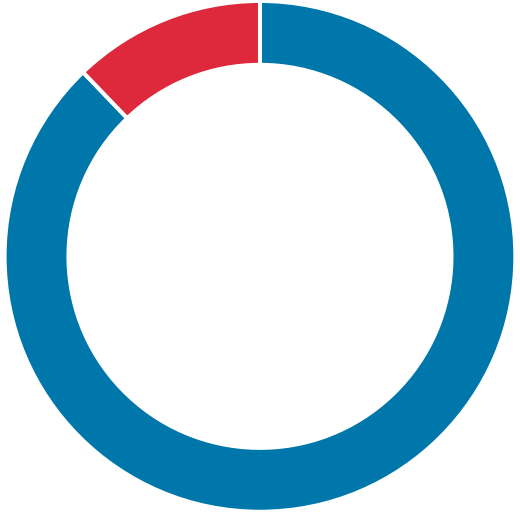
Otevřené emaily
42,85%



Kliknutí na odkaz
19,96%



Zadaná data
12,18%



PhishTest – ukázka

st 16.11.2022 8:14

AB

Expirace Hesla

Komu Ondrej Malík

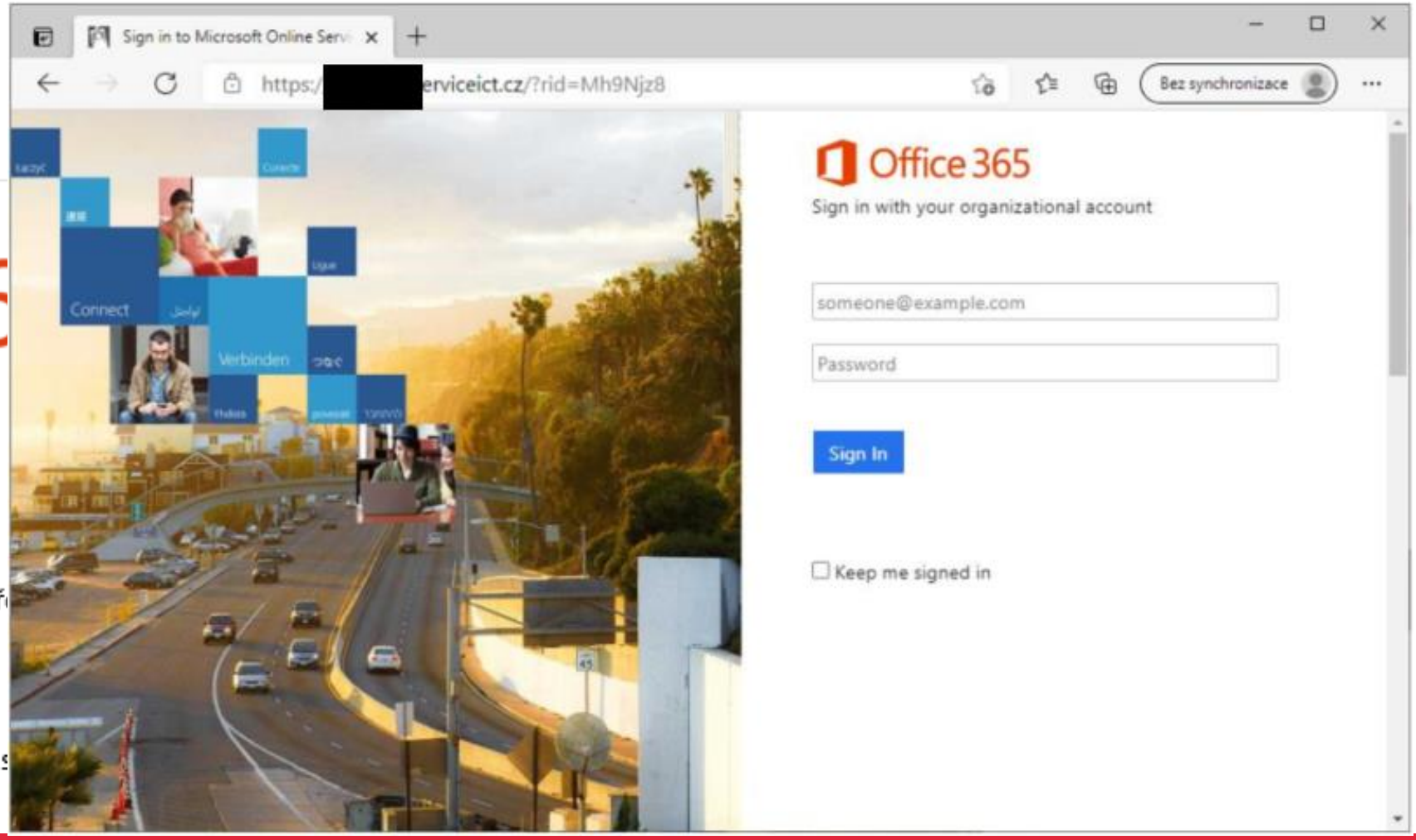
Office 36

Vážený uživateli,

Došlo k expiraci Vašeho hesla k Office365.
Pro obnovení hesla se prosím přihlaste prostř

Microsoft Office 365 Team!

Další informace k resetování hesla a ochraně s



Jak služba funguje?

- Testování je prováděno pomocí e-mailů, které sim
- Vytvoření scénáře útoku - vizuálu podvodného e-r
- Spuštění kampaně rozesláním vybraných podvodr
- Sledování průběhu kampaně po smluvenou dobu.
- Sběr dat a jejich vyhodnocení.
- Závěrečná zpráva obsahující podrobné zhodnocen
  posílení 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 phisingového **emailu obsahujícího malware přílohu.**

Úroveň 3

Na míru

Otestování uživatelů dle Vašich specifických požadavků a přání.

Kontaktujte nás

Úroveň 4

Aug 19, 202

August 21st, 2023 August 8th, 2023

SonicWALL G(0Day) Microsoft GitHub Dev-Containers Improper Privilege Management Privilege Escalation Vulnerability

ZDI-23-1154
ZDI-CAN-2091

ZDI-23-1044
ZDI-CAN-20784

sfewer-r

Code

CVE ID

CVSS SC

AFFECTE

AFFECTE

VULNER

ADDITIO

CVE ID	
CVSS SCORE	9.9, (AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)
AFFECTED VENDORS	Microsoft
AFFECTED PRODUCTS	GitHub
VULNERABILITY DETAILS	This vulnerability allows remote attackers to escalate privileges on affected installations of Microsoft GitHub. Authentication is required to exploit this vulnerability. The specific flaw exists within the configuration of Dev-Containers. The application does not enforce the privileged flag within a devcontainer configuration. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the hypervisor.
ADDITIONAL DETAILS	04/06/23 – ZDI reported the vulnerability to the vendor.

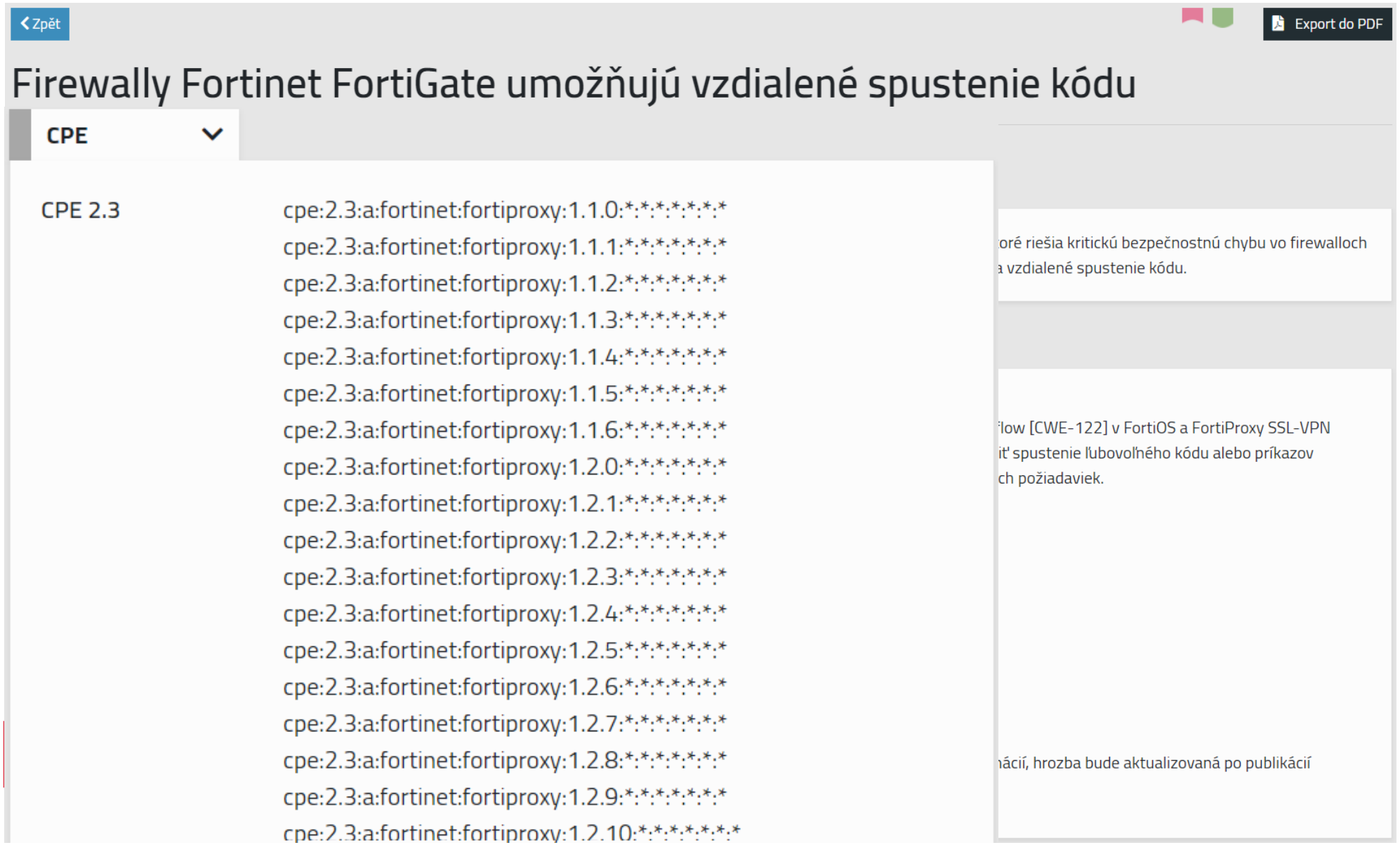
Networking
address mul
remote code

The four vul
affect all ver

"By chaining
able to remo
2023.

Virtuální bezpečnostní analytik

- Výsledek nepřetržité práce týmu 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 týmu


Zpět
Export do PDF
Firewally Fortinet FortiGate umožňujú vzdialené spustenie kódu
CPE
CPE 2.3
cpe:2.3:a:fortinet:fortiproxy:1.1.0:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:1.1.1:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:1.1.2:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:1.1.3:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:1.1.4:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:1.1.5:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:1.1.6:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:1.2.0:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:1.2.1:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:1.2.2:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:1.2.3:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:1.2.4:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:1.2.5:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:1.2.6:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:1.2.7:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:1.2.8:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:1.2.9:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:1.2.10:*:*:*:*:*:*:*
oré riešia kritickú bezpečnostnú chybu vo firewalloch
a vzdialené spustenie kódu.
low [CWE-122] v FortiOS a FortiProxy SSL-VPN
it' spustenie ľubovoľného kódu alebo príkazov
ch požiadaviek.
ácií, hrozba bude aktualizovaná po publikácií

Náprava

Ak je funkcia SSL-VPN povolená, spoločnosť Fortinet odporúča zákazníkom, aby okamžite vykonali aktualizáciu na najnovšiu verziu firmwaru. Ak zákazník nepoužíva protokol SSL-VPN, riziko tohto problému sa zmierňuje - spoločnosť Fortinet však stále odporúča aktualizáciu.

Opatření

Trellix IPS Emergency UDS pre CVE-2023-2868, CVE-2023-27997, CVE-2023-34362, CVE-2023-20887

Trellix IPS Emergency UDS pre CVE-2023-2868, CVE-2023-27997, CVE-2023-34362, CVE-2023-20887

Zpět

Základní údaje

Ověřenost	Testováno	Přidáno	20.6.2023 13:40
Úplnost reportu	plný	Aktualizováno	20.6.2023 16:08
Vytvořil	Michal Mezera		

Přílohy

Příloha (1)
Příloha (2)

Zdroje

https://kcm.trellix.com/corporate/index?page=content&id=KB55447

Popis

POZNÁMKA: Články UDS sú **registrované** články a vyžadujú prihlásenie do ServicePortal.

Signatúry definované používateľom (UDS) sa poskytujú ako okamžité riešenie bezpečnostného upozornenia. UDS je určený na pokrytie známych aspektov hrozby a nemusí pokrývať všetky varianty. Niekedy môžu vydania UDS generovať nesprávnu identifikáciu.

Stiahnutie UDS

1. Kliknite na odkaz v článku databázy znalostí pre UDS, ktorý je potrebný stiahnuť.
2. Stiahnite súbor .zip pripojený k článku, ktorý obsahuje UDS.
3. Rozbaľte stiahnutý súbor .zip.

Import UDS do správcu

1. Prihláste sa do aplikácie Manager.
2. Kliknite na položku Policy, Intrusion Prevention, Policy Types.
- Pre Manager 9.x kliknite na položku IPS Policies.
- Pre Manager 10.x a novšie verzie vrátane verzie 11.x kliknite na položku IPS.
3. Kliknite na odkaz Custom Attacks v dolnej časti ľavého panela.
4. Kliknite na položku Other Actions a potom na položku Import.
5. Kliknite na tlačidlo Browse a vyberte súbor Emergency_UDS_xxx.zip.
6. Zrušte výber nasledujúcich položiek:
- Import Snort Rules
- Import Snort Macros
- Import Snort Classifications
7. Kliknite na tlačidlo Import.
8. Skontrolujte, či počet úspešne importovaných UDS nie je nulový (1 alebo vyšší).

Aplikujte UDS na každý senzor jeden po druhom

1. Otvorte aplikáciu Manager.
2. Prejdite na položku Devices.
3. V ľavom navigačnom paneli vyberte kartu Devices.
4. Z rozbaľovacieho zoznamu vyberte Senzor, do ktorého chcete poslať aktualizáciu.
5. Kliknite na tlačidlo Deploy Pending Changes. Táto možnosť už musí byť vybratá.
6. Ak chcete spustiť aktualizáciu snímača, kliknite na tlačidlo Update/Deploy.

Ak chcete použiť UDS na všetky Senzory

1. Otvorte aplikáciu Manager.
2. Prejdite na položku Devices.
3. V ľavom navigačnom paneli vyberte kartu Global.
4. Kliknite na položku Deploy Pending Changes. Každý snímač, ktorý vyžaduje aktualizáciu, musí byť vybraný.
5. Ak chcete spustiť aktualizáciu Senzorov, kliknite na tlačidlo Update/Deploy.

COMGUARD

Stěžejní funkcionality v ThreatGuard

- **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 Trellix ATD** – nahrajete neznámý soubor nebo URL adresu skrze ThreatGuard do McAfee, kde se otestuje a řekne Vám, jestli je v pořádku nebo kritický
- **Integrace s Whalebone Immunity** – zjistěte reputaci domény prostřednictvím portálu ThreatGuard
- **ThreatManager** – zpracovávejte jednotlivé hrozby v týmu

Detail projektu

Cisco/Fortinet

Upravit

Popis projektu	Hrozby evidované na Cisco/Fortinet
Vytvořeno	11.09.2023 09:51:40
Termín	Projekt nemá termín
Filtry	Cisco/Fortinet
Režim filtru	Dynamický
Autor projektu	Roman Jiráček
Členové	• Roman Jiráček • Jakub Mazal
Termín	Projekt nemá termín

Hrozby projektu 5/297 | **Komentáře** 0

Cisco produkty jsou náchylné na DoS

Vendoři: Cisco
Štítky:
Závažnost: vysoká
Typy: DoS

Aktualizováno 7.9.2023

Spuštění libovolného kódu v Cisco Small Business routerech z 6. 9. 2023

Vendoři: Cisco
Štítky:
Závažnost: střední
Typy: vzdálené spuštění kódu

Aktualizováno 7.9.2023

DoS útok v Cisco Identity Services Engine z 6. 9. 2023

Vendoři: Cisco
Štítky:
Závažnost: vysoká
Typy: DoS

Aktualizováno 7.9.2023

Zpět k projektu

Export do PDF

Spuštění libovolného kódu v Cisco Small Business routerech z 6. 9. 2023

Základní údaje

ID	2792	Přidáno	7.9.2023 13:26
Úplnost reportu	plný	Aktualizováno	7.9.2023 13:54
Typy	vzdálené spuštění kódu	Geolokace	global
		Autor	COMGUARD a.s.
Závažnost	střední		

CVSS závažnost	6.5
CVSS	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N
CVE	CVE-2023-20250
Zdroje	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-stack-SHYv2f5N?vs_f=Cisco%20Security%20Advisory&vs_cat=Security%20Intelligence&vs_type=RSS&vs_p=Cisco%20Small%20Business%20RV110W,%20RV130,%20RV130W,%20and%20RV215W%20Routers%20Stack%20Overflow%20Vulnerability&vs_k=1
Vendoři	Cisco

Krátký popis

Byla objevena zranitelnost v routerech Cisco Small Business RV110W, RV130, RV130W, a RV215W, která umožňuje útočníkovi spustit na napadeném zařízení libovolný kód.

Detailní popis

Uvedená zranitelnost existuje z důvodu nesprávné validace požadavků odeslaných na webové rozhraní pro správu, čehož může útočník zneužít odesláním jím vytvořeného požadavku na zmíněné webové rozhraní, což mu umožní spustit libovolný kód s oprávněními *roota* na napadeném zařízení. Pro úspěšné zneužití této zranitelnosti musí mít útočník nejprve k dispozici validní přihlašovací údaje administrátora napadeného zařízení.

Náprava

Vendor Cisco nevydal a nevydá žádné nové aktualizace zmíněných routerů popsaných v tomto reportu, jelikož uvedeným routerům končí životnost. Uživatelům doporučujeme sledovat upozornění na konec životnosti zmíněných produktů na následujícím odkazu:

End-of-Sale and End-of-Life Announcement for the Cisco Small Business RV Series Routers (selected models)

Bližší informace jsou k dispozici na odkazu v sekci Zdroje tohoto reportu.

Opatření

Omezení přístupu k systému

Komentáře k hrozbě

Váš komentář

Odeslat

Roman Jiráček 11.9.2023 | 09:57
Vyřešeno!

ThreatGuard LITE

- Databáze ThreatGuard
- CVE databáze
- POUZE jeden aktivní filtr nad oběma databázemi
- Náprava dané hrozby – k dispozici jsou uživatelům pouze obecné nápravy pro jednotlivé hrozby
- Grafy dle CVE databáze per jednotlivý měsíc

ThreatGuard PRO

- Databáze ThreatGuard
- CVE databáze
- Portál je i v AJ
- Neomezený počet aktivních filtrů nad oběma databázemi
- Komplexní nápravy jednotlivých hrozeb, vč. opatření (workaround, konfigurace apod.
- Grafy dle CVE databáze per jednotlivý měsíc
- Integrovaný CSIRT CZ a SK
- Analýza Sandbox
- Analýza Whalebone Immunity
- Threat Manager

ThreatGuard ULTRA

- Databáze ThreatGuard
- CVE databáze
- Portál je i v AJ
- Neomezený počet aktivních filtrů nad oběma databázemi
- Komplexní nápravy jednotlivých hrozeb, vč. opatření (workaround, konfigurace apod.
- Grafy dle CVE databáze per jednotlivý měsíc
- Integrovaný CSIRT CZ a SK
- Analýza Sandbox
- Analýza Whalebone Immunity
- Threat Manager
- Real-time chat – podpora expertního týmu přímo v platformě ThreatGuard

COMGUARD

cyber security masters

Děkujeme za pozornost!