COMGUARD

cyber security masters

Novinky 2024

ThreatGuard a COMGUARD

Roman Jiráček, Senior Account & Vendor Manager

20.09.2024

COMGUARD

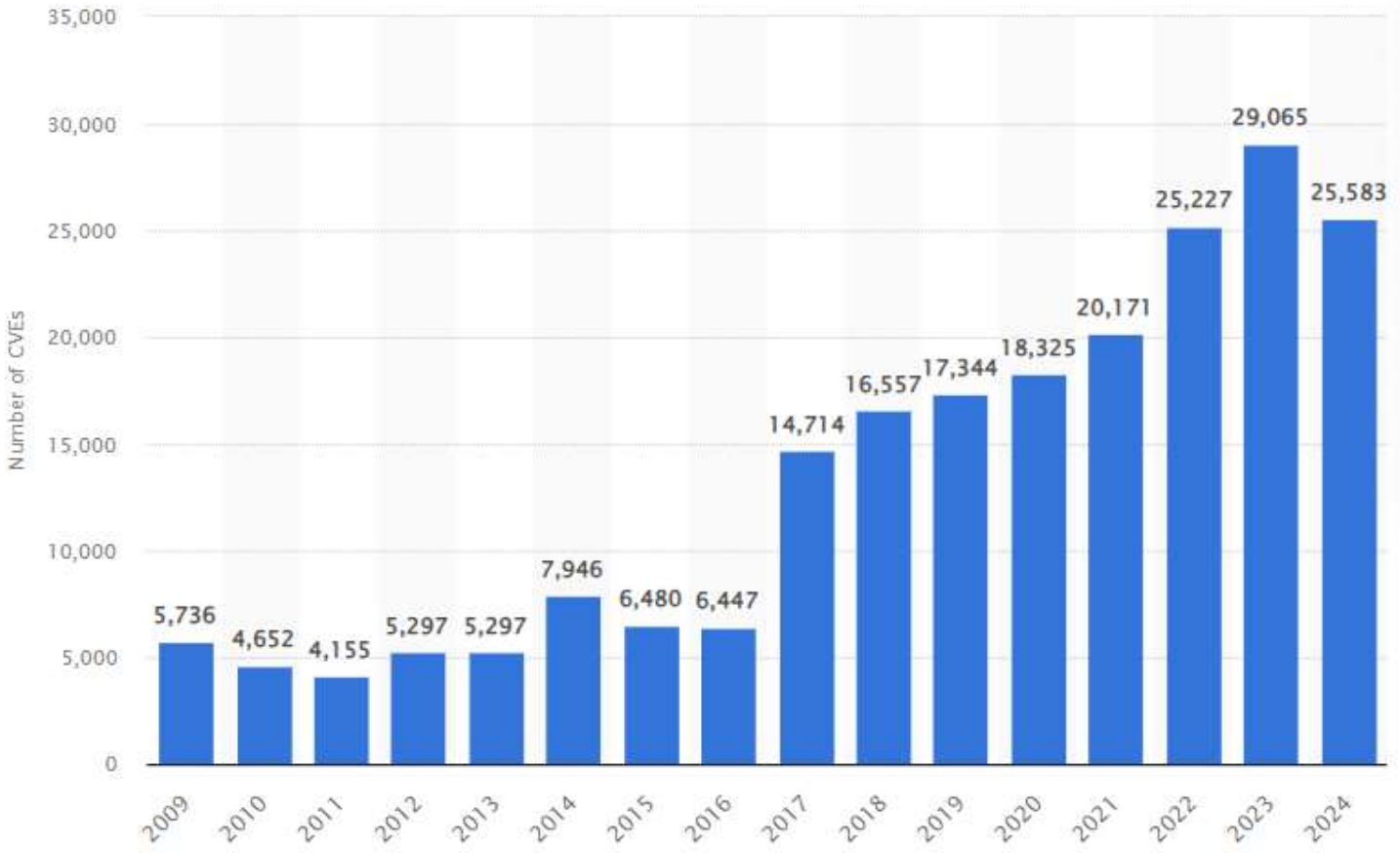
Informace

Technologie

Uživatelé

COMGUARD

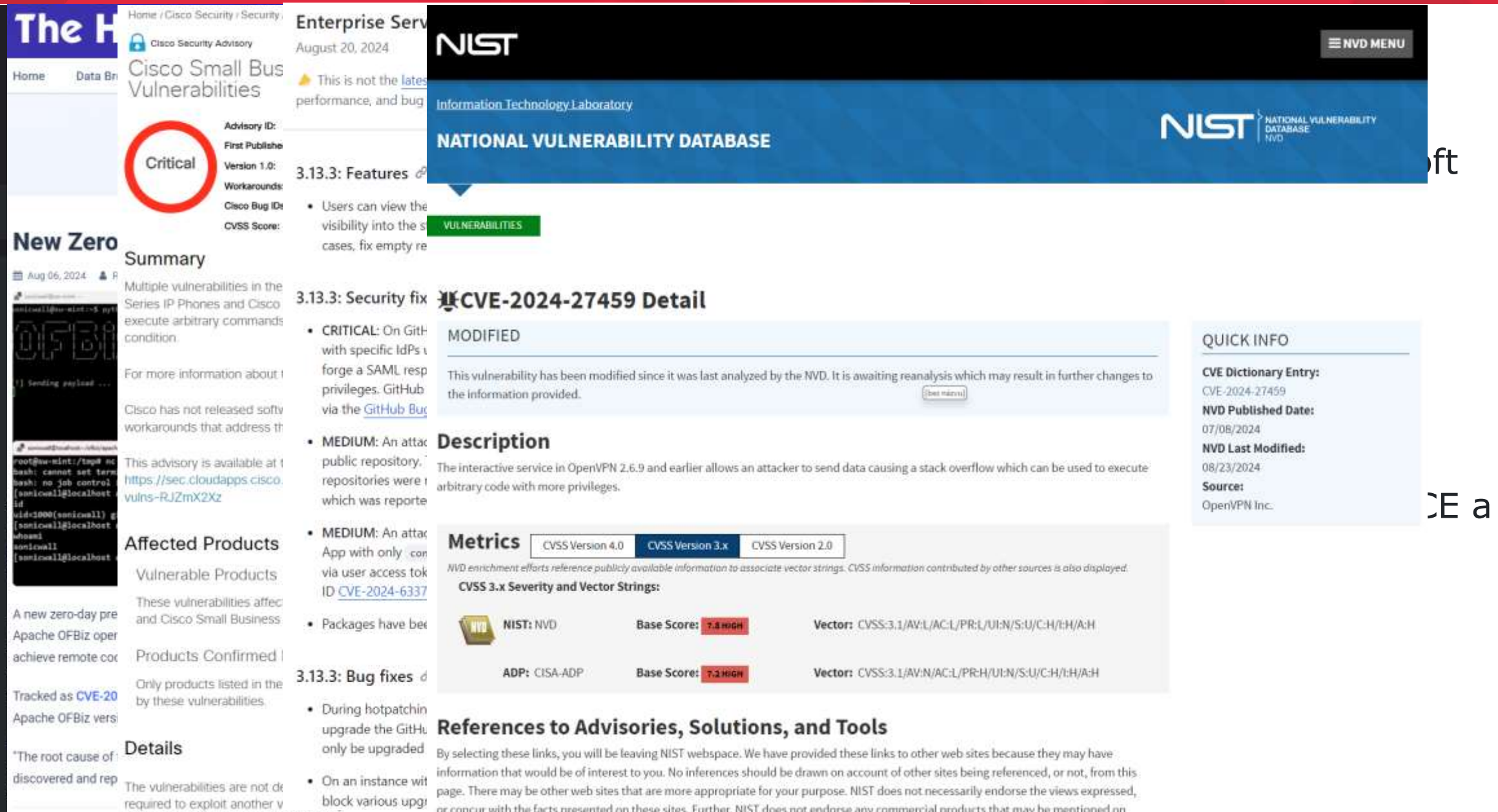
Number of common IT security vulnerabilities and exposures (CVEs) worldwide from 2009 to 2024 YTD



COMGUARD

Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks

Region	Avg weekly attacks per org	YoY Change
Africa	2960	+37%
Latin America	2667	+53%
APAC	2510	+23%
Europe	1367	+35%
North America	1188	+17%



The H

Home / Cisco Security / Security

Cisco Security Advisory

Cisco Small Bus
Vulnerabilities

Critical

Advisory ID:
First Publishe
Version 1.0:
Workarounds:
Cisco Bug IDs
CVSS Score:

Summary

Multiple vulnerabilities in the
Series IP Phones and Cisco
execute arbitrary commands
condition

For more information about

Cisco has not released softv
workarounds that address th

This advisory is available at t
https://sec.cloudapps.cisco.
vulns-RJZmX2Xz

Affected Products

Vulnerable Products

These vulnerabilities affec
and Cisco Small Business

Products Confirmed

Only products listed in the
by these vulnerabilities

Details

The vulnerabilities are not de
required to exploit another v

Enterprise Serv

August 20, 2024

This is not the lates
performance, and bug

3.13.3: Features

- Users can view the
visibility into the s
cases, fix empty re

3.13.3: Security fix

- CRITICAL: On GitH
with specific IdPs
forge a SAML resp
privileges. GitHub
via the GitHub Bug
- MEDIUM: An attac
public repository.
repositories were
which was reporte
- MEDIUM: An attac
App with only con
via user access tok
ID CVE-2024-6337
- Packages have bee

3.13.3: Bug fixes

- During hotpatchin
upgrade the GitHu
only be upgraded
- On an instance wit
block various upgr

NIST

NVD MENU

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

CVE-2024-27459 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

The interactive service in OpenVPN 2.6.9 and earlier allows an attacker to send data causing a stack overflow which can be used to execute arbitrary code with more privileges.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD — **Base Score:** 7.8 HIGH — **Vector:** CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

ADP: CISA-ADP — **Base Score:** 7.3 HIGH — **Vector:** CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed,

QUICK INFO

CVE Dictionary Entry:
CVE-2024-27459
NVD Published Date:
07/08/2024
NVD Last Modified:
08/23/2024
Source:
OpenVPN Inc.

New Zero

Aug 06, 2024

A new zero-day pre
Apache OFBiz oper
achieve remote coc

Tracked as CVE-20
Apache OFBiz versi

"The root cause of
discovered and rep

ft

CE a

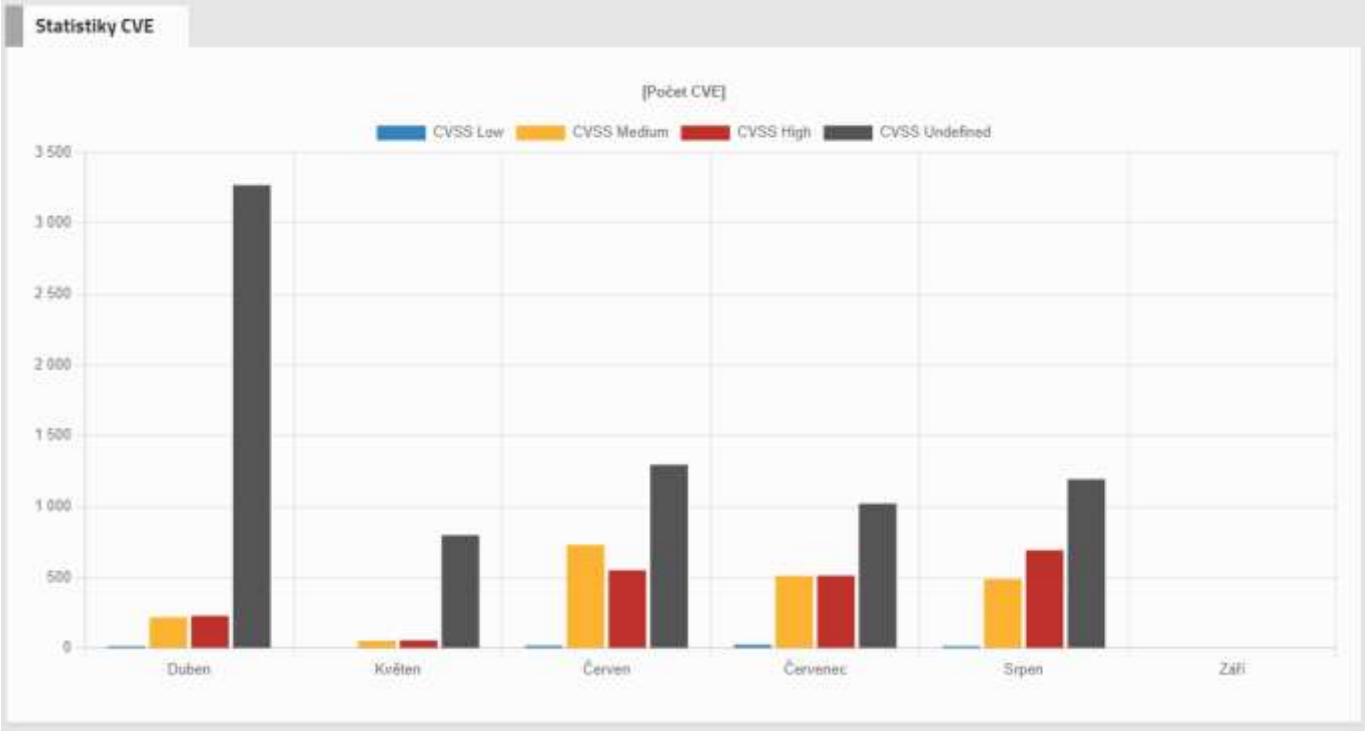
Virtuální bezpečnostní analytik

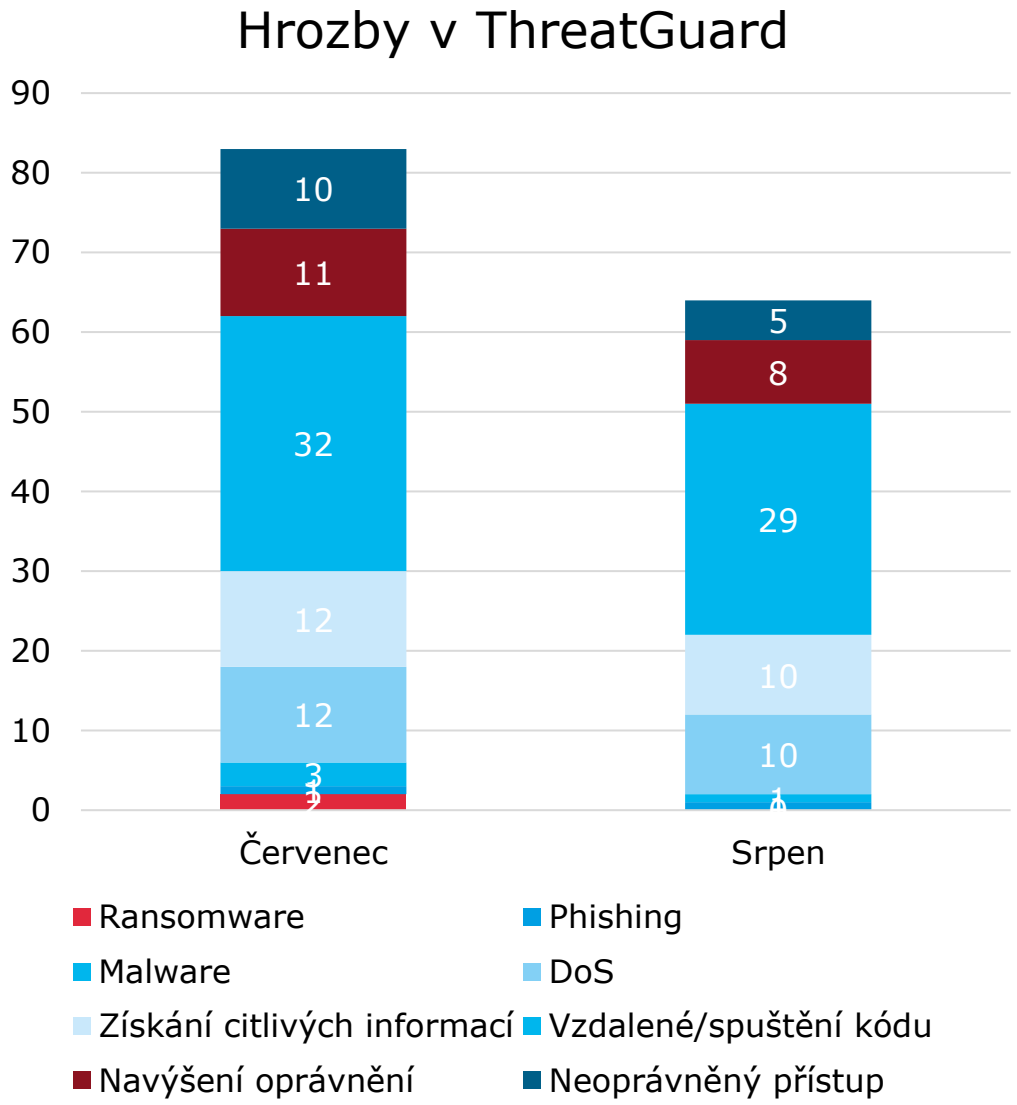
- Výsledek nepřetržité práce týmu bezpečnostních analytiků
  - Databáze aktuálních hrozeb pro Vaše IT
  - Prověřené návrhy nápravných opatření
- Možnost filtrace hrozeb dle Vašich aktiv
- Dostupné formou webového portálu s notifikacemi
  - Chat s podporou expertního týmu

Hrozby v ThreatGuard

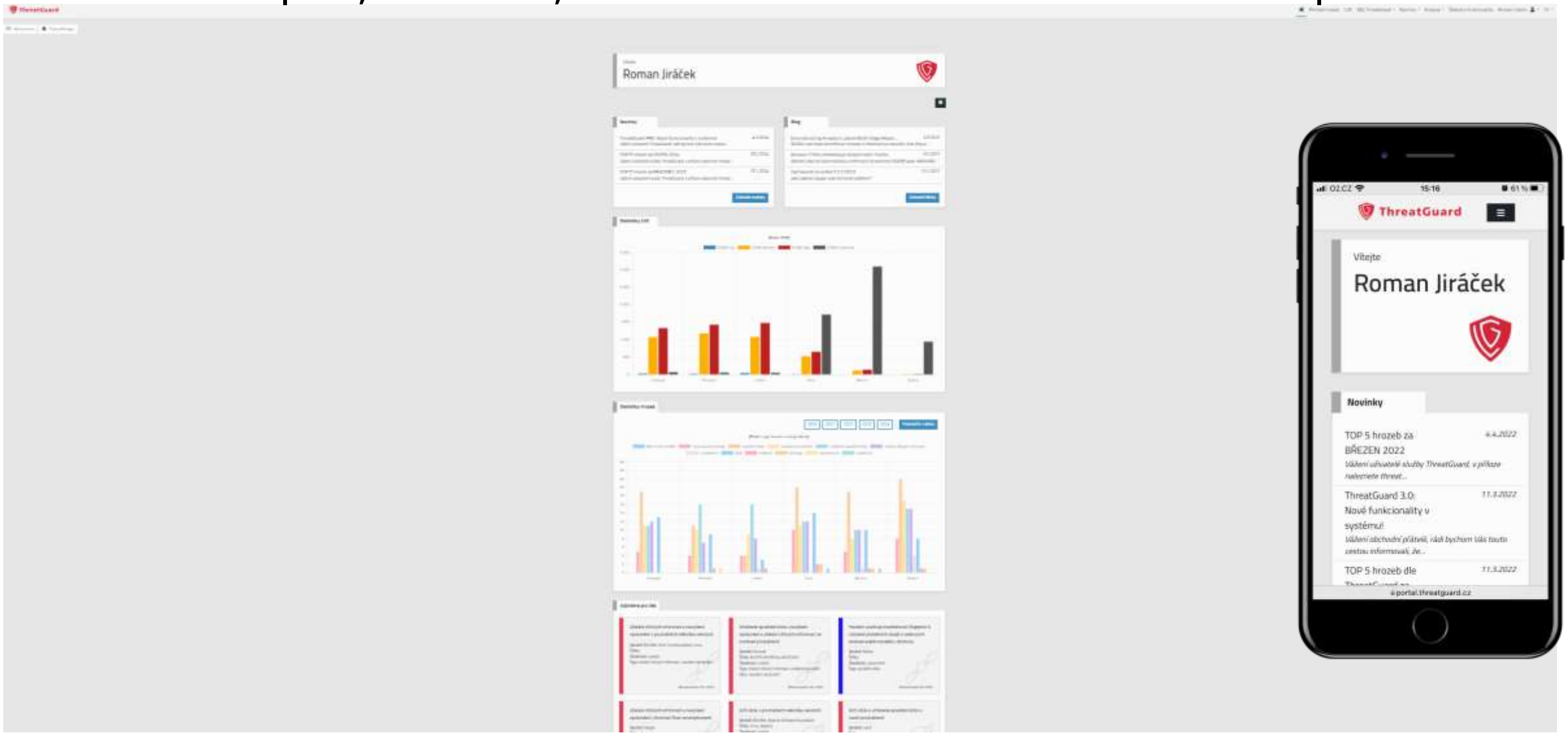
Granulární členění hrozeb:

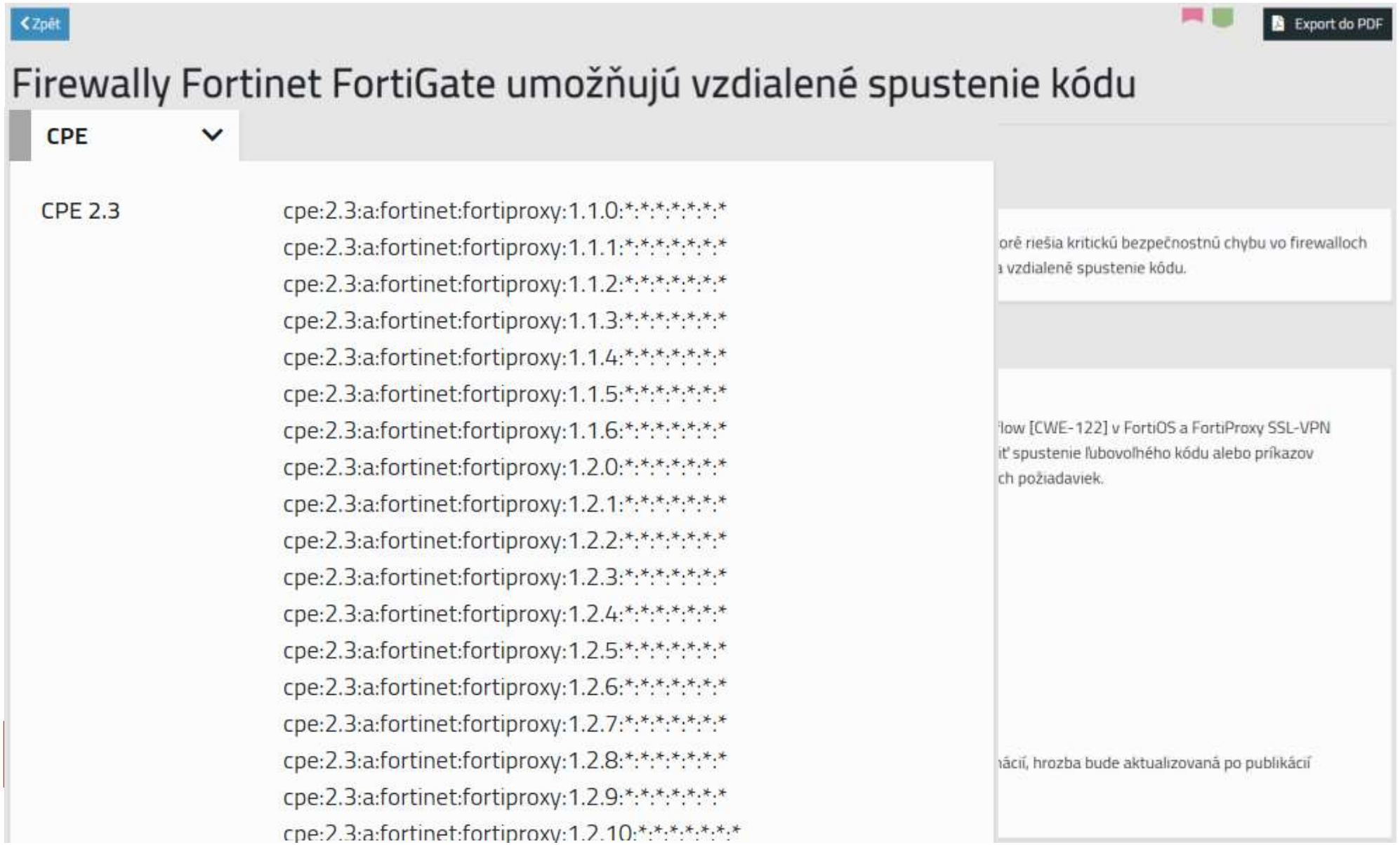
- Ransomware
- Malware
- Phishing
- DoS
- Získání citlivých informací
- Navýšení oprávnění
- Vzdálené spuštění kódu
- Spuštění kódu
- Neoprávněný přístup





Stále dostupná, aktuální, strukturovaná databáze hrozeb a opatření




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:*:*:*:*:*:*:*
orě riešia kritickú bezpečnostnú chybu vo firewalloch
a vzdialeně 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

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 Trellix, 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

COMGUARD

ThreatGuard – Threat Manager

Cisco/Fortinet

Export do PDF | Upravit

Popis projektu	Hrozby evidované na Cisco/Fortinet
Vytvořeno	11.09.2023 09:51:40
Termín	Projekt nemá termín
Filtry	Cisco, Cisco/Fortinet, Fortinet
Režim filtru	Dynamický
Autor projektu	Roman Jiráček
Členové	• Roman Jiráček • Jakub Mazal
Termín	Projekt nemá termín
Celkem hrozeb	339
Vyřešené hrozby	7

Vyhledejte filtrem níže

Hledat

Filtr

Hrozby projektu 332 | Vyřešené hrozby 7 | Komentáře 0

Seřadit podle Přidáno ○ Vzestupně ◉ Sestupně Seřadit

Vzdálené spuštění kódu, navýšení oprávnění a získání citlivých informací ve Fortinet produktech

Vendoři: Fortinet
Štítky: FortiOS, FortiProxy, FortiClient
Závažnost: vysoká
Typy: získání citlivých informací, vzdálené spuštění kódu, navýšení oprávnění

Aktualizováno 10.4.2024

Vzdálené spuštění kódu, navýšení oprávnění a získání citlivých informací ve Fortinet produktech

Vendoři: Fortinet
Štítky: FortiOS, FortiProxy, FortiClient
Závažnost: vysoká
Typy: získání citlivých informací, vzdálené spuštění kódu, navýšení oprávnění

Aktualizováno 10.4.2024

Získání citlivých informací a neoprávněný přístup v Cisco produktech

Vendoři: Cisco
Štítky:
Závažnost: vysoká
Typy: získání citlivých informací, neoprávněný přístup

Aktualizováno 4.4.2024

Základní údaje

ID	3149	Přidáno	10.4.2024 10:00
Úplnost reportu	plný	Aktualizováno	10.4.2024 10:17
Typy	získání citlivých informací, vzdálené spuštění kódu, navýšení oprávnění	Geolokace	global
		Autor	COMGUARD a.s.
Závažnost	vysoká		

CVSS závažnost	9.6
CVSS	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
CVE	CVE-2023-45588 CVE-2024-31492 CVE-2023-41677 CVE-2023-45590
Zdroje	https://www.cisa.gov/news-events/alerts/2024/04/09/fortinet-releases-security-updates-multiple-products https://www.fortiguard.com/psirt/FG-IR-23-345 https://www.cybersecurity-help.cz/vdb/SB2024040962 https://www.fortiguard.com/psirt/FG-IR-23-493 https://www.cybersecurity-help.cz/vdb/SB2024040954 https://www.fortiguard.com/psirt/FG-IR-23-087 https://www.cybersecurity-help.cz/vdb/SB2024040961
Vendoři	Fortinet
Štítky	FortiOS FortiProxy FortiClient

Náprava

Vendor Fortinet vydal aktualizace, které jež zmíněné zranitelnosti opravují. Bližší informace jsou k dispozici na odkazech v sekci Zdroje tohoto reportu.
Administrátorům doporučujeme, aby příslušné aktualizace nainstalovali co nejdříve.

Opatření

Neotevírat odkazy v e-mailech, SMS a MMS zprávách.

Komentáře k hrozbě

Váš komentář

Odeslat

Krátký popis

Byly objeveny čtyři zranitelnosti ve Fortinet FortiClientMac, FortiOS, FortiProxy a FortiClientLinux umožňující útočníkovi vzdálené spuštění kódu, navýšení oprávnění a získání citlivých informací na těchto produktech.

Detailní popis

Jedná se o tyto zranitelnosti:

CVE-2023-45588 & CVE-2024-31492

Tyto zranitelnosti existují kvůli chybějícímu ověření konfiguračního souboru v instalačním programu softwaru, což může lokální útočník zneužít k vytvoření speciálně vyrobeného konfiguračního souboru do adresáře /tmp a spustit tak libovolný kód se zvýšenými právy.

CVE-2023-41677

Uvedená zranitelnost existuje z důvodu nedostatečně chráněného pověření, čehož může vzdálený útočník zneužít, aby přiměl uživatele k návštěvení speciálně vytvořené webové stránky, prostřednictvím SSL-VPN a získal tak adminstrátorské cookies.

CVE-2023-45590

Daná zranitelnost se vyskytuje v klientovi FortiClient kvůli nebezpečné konfiguraci node.js, což může vzdálený útočník zneužít, aby přiměl uživatele k návštěvě speciálně vytvořené webové stránky a spustit tak v systému libovolný kód.

Úspěšné zneužití této zranitelnosti může vést k úplné kompromitaci zranitelného systému.

CS

COMGUARD

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

COMGUARD

Novinky v portfoliu COMGUARD a.s.

Cyber Threat Intelligence & Risk Quantification

- Rok založení = 2011
- Lokace = USA, Arlington
- Počet zaměstnanců do 200
- Web: www.threatconnect.com

Threat Intelligence Operations Platform

- Vysoce škálovatelné a flexibilní řešení pro provozování zpravodajství o kybernetických hrozbách
- Shromažďuje a obohacuje informace o hrozbách na jediném místě
- Analyzovuje informace, určuje priority a zasahuje proti nejrelevantnějším hrozbám pomocí AI a ML
- Automatizace a robustní operability napříč nástroji v organizaci
- Umožňuje týmům pro kybernetickou bezpečnost identifikovat, zkoumat a reagovat na hrozby efektivněji a přesněji

Risk Quantifier

- Umožňuje podnikům efektivně kvantifikovat kybernetické riziko z pohledu nákladů pro danou společnost
- RQ je jedinou platformou v oboru pro automatizovanou kvantifikaci kybernetických rizik založenou na datech a strojovém učení
- Kombinuje velké datové sady s vlastními modely strojového učení
- Automatizuje produkci dat o rizicích
- S ThreatConnect RQ společnosti upřednostňují investice na základě skutečného finančního rizika
- Napomáhá efektivně komunikovat bezpečnostní strategie se výkonnými týmy a managementem společnosti

COMGUARD

cyber security masters

Děkujeme za pozornost

Roman Jiráček
E-mail: roman.jiracek@comguard.cz
Tel.: +420 770 127 080