

Mam UTM
i czy jestem
bezpieczny?

NETIA
netianext

FORTINET®

 EXCLUSIVE
NETWORKS

Trochę historii...

Na początku był....

Fortigate.



NETIA
netianext



Trochę historii...

2017 – powstanie dedykowanego zespołu w Netii

2018 – pierwszy zarządzany przez **Netię Fortigate**

-
-
-

2023 – ponad 1000 utrzymywanych usług



O nas

13 inżynierów
(zaczynaliśmy od **2** osób)
24/7

Certyfikaty w Dziale:



UTM a bezpieczeństwo

- „Dziurawy soft”
- Brak wsparcia
- Domyślna konfiguracja
- „Płaska sieć”
- „Przekierowania” portów
- Brak przeglądów konfiguracji
- Brak wiedzy i doświadczenia



UTM a bezpieczeństwo

sekurak

SZKOLENIA | KSIĄŻKA | AKTUALNOŚCI | TEKSTY | KONTAKT | AUDYTY | O NAS

Wprowadzenie do bezpieczeństwa IT - zamów nową książkę sekuraka w preorderze.

Nowa krytyczna podatność w Fortigate (precyzyjniej: FortiOS/FortiProxy). Łatajcie się.

14 LIPCA 2023, 09:06 | W BIEGU | KOMENTARZY 10

TAGI: BUFFER OVERFLOW

Tym razem mamy podatność klasy buffer overflow, która może być wykorzystana bez uwierzytelnienia / zdalnie:

FortiOS/FortiProxy - Proxy mode with deep inspection - Stack-based buffer overflow

Po tym krótkim opisie mniej więcej widać gdzie jest problem. Atakujący wysła odpowiednią (złośliwą) komunikację, jest ona analizowana przez urządzenie, co powoduje... wykonanie kodu (RCE) na nim. Producent opisuje to tak:

A stack-based overflow vulnerability [CVE-124] in FortiOS & FortiProxy may allow a remote attacker to execute arbitrary code or command via crafted packets reaching proxy policies or firewall policies with proxy mode alongside SSL deep packet inspection.

Nadzieją jest to, że nie wszyscy muszą mieć włączoną ww. opcję. Podatne wersje OS

FortiOS 7.2.0 -> 7.2.3
FortiOS 7.0.0 -> 7.0.10
FortiProxy 7.2.0 -> 7.2.2
FortiProxy 7.0.0 -> 7.0.9

Łatajcie się.

NOWA KSIĄŻKA SEKURAKA!

Nowa książka od SEKURAKA

WPROWADZENIE DO BEZPIECZEŃSTWA IT

18 autorów 942 strony
18 rozdziałów pełny kolor

CERT Polska
@CERT_Polska · Obserwuj

!!! Ostrzegamy przed krytyczną podatnością w urządzeniach #FortiGate SSL VPN. Łatka dla CVE-2023-27997 jest już dostępna, a my zachęcamy do jej niezwłocznego stosowania, bo podatność może być i będzie wykorzystywana podczas ataków #ransomware.

10:45 AM · 12 cze 2023

52 Odpowiedz Udostępnij

Przeczytaj 1 odpowiedź

Home / PSIRT / FG-IR-22-398

PSIRT Advisories

FortiOS - heap-based buffer overflow in sslvpn

IR Number: FG-IR-22-398

Date: Dec 12, 2022

Severity: Critical

CVSSv3 Score: 9.3

Impact: Execute unauthorized code or commands

CVE ID: CVE-2022-42475

Affected Products: FortiProxy : 7.2.1, 7.2.0, 7.0.7, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0, 2.0.6, 2.0.5, 2.0.7, 2.0.8, 2.0.9, 2.0.4, 2.0.3, 2.0.2, 2.0.11, 2.0.10.

Summary:
A heap-based buffer overflow vulnerability [CVE-122] in FortiOS SSL-VPN may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests.

Exploitation status:
Fortinet is aware of an instance where this vulnerability was exploited in the wild, and recommends immediately validating your systems against the following indicators of compromise:

Multiple log entries with:
Logdesc="Application crashed" and msg="[...] application:sslvpn,[...], Signal 11 received, Backtrace: [...]"

CERT.PL NASK

O nas Aktualności Baza wiedzy Dla ekspertów

Zgłoś incydent

Fortinet opublikował informację o krytycznej podatności CVE-2022-42475 pozwalającej na zdalne wykonanie kodu bez uwierzytelnienia w module SSL-VPN (sslvpn) dla FortiOS. **Podatność była aktywnie wykorzystywana w atakach jeszcze zanim jej istnienie zostało ujawnione.** Ze względu na charakter podatności, wszystkim administratorom urządzeń Fortinet zalecamy natychmiastowe zastosowanie się do poniższych rekomendacji.

Podatne wersje i rekomendacje aktualizacji

- FortiOS wersje od 7.2.0 do 7.2.2 włącznie
 - Należy zaktualizować minimum do wersji 7.2.3
- FortiOS wersje od 7.0.0 do 7.0.8 włącznie
 - Należy zaktualizować minimum do wersji 7.0.9
- FortiOS wersje od 6.4.0 do 6.4.10 włącznie
 - Należy zaktualizować minimum do wersji 6.4.11
- FortiOS wersje od 6.2.0 do 6.2.11 włącznie
 - Należy zaktualizować minimum do wersji 6.2.12
- FortiOS wersje od 6.0.0 do 6.0.15 włącznie
 - Należy zaktualizować minimum do wersji 6.0.16
- FortiOS wersje od 5.6.0 do 5.6.14 włącznie
 - Należy zaktualizować minimum do wersji 6.0.16
- FortiOS wersje od 5.4.0 do 5.4.13 włącznie
 - Należy zaktualizować minimum do wersji 6.0.16
- FortiOS wersje od 5.2.0 do 5.2.15 włącznie
 - Należy zaktualizować minimum do wersji 6.0.16
- FortiOS wersje od 5.0.0 do 5.0.14 włącznie

UTM a bezpieczeństwo

From: CERT Polska via RT <cert@cert.pl>
Sent: Thursday, June 22, 2023 7:29 PM
To: [REDACTED]
Subject: [EXT] [CERT.PL #2407698] [PILNE] Powiadomienie CERT Polska/CSIRT NASK w sprawie krytycznej podatności CVE-2023-27997

Szanowni Państwo
jesteśmy zespołem reagowania na incydenty bezpieczeństwa informatycznego CERT Polska. Zespołowi CERT Polska zostały powierzone obowiązki CSIRT NASK wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560).

Ponownie kontaktujemy się z Państwem, ponieważ z wykonanego przez nas skanowania wynika, że w Państwa sieci nadal znajdują się hosty z podatną wersją oprogramowania firmy Fortinet. W przypadku, gdy urządzenie to należy do Państwa klientów, prosimy o przekazanie tej wiadomości do odpowiedniego podmiotu. Podatne instancje znajdują się pod następującymi adresami:

ip:port
8 [REDACTED] 43
7 [REDACTED] 443
7 [REDACTED] 6443
8 [REDACTED] 443
8 [REDACTED] :6443
8 [REDACTED] 443
7 [REDACTED] 43
4 [REDACTED] 4433
7 [REDACTED] 443
8 [REDACTED] 443
7 [REDACTED] 443
7 [REDACTED] 443
3 [REDACTED] 2:8443
2 [REDACTED] 4:444

Nasz zespół otrzymał informację o krytycznej podatności CVE-2023-27997 występującej w usłudze SSL-VPN urządzeń Fortigate z systemem FortiOS w wersjach poniżej 6.0.17, 6.2.15, 6.4.13, 7.0.12 oraz 7.2.5. Jeśli, zgodnie z naszymi informacjami, posiadają Państwo takie urządzenia, zalecamy bezzwłoczne zainstalowanie najnowszych aktualizacji wydanych przez producenta po 8 czerwca 2023, gdyż wspomniana podatność może posłużyć do prób ataków, w tym ataków z użyciem ransomware, na Państwa infrastrukturę.

Oficjalny komunikat firmy Fortigate zawierający opis podatności można znaleźć na stronie producenta <https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign>. Na ten moment wiadomo, że luka umożliwia zdalne wykonywanie kodu bez konieczności dokonywania uwierzytelniania i jest aktywnie wykorzystywana do przeprowadzania ataków typu z wykorzystaniem ransomware.

Prosimy o potwierdzenie otrzymania wiadomości. Jeżeli wskazane w zawiadomieniu hosty zostały już zaktualizowane, również prosimy o informację wraz ze wskazaniem, do jakiej wersji - umożliwi to ograniczenie fałszywych alarmów w przyszłości. W przypadku pytań lub wątpliwości pozostajemy do dyspozycji.

Z poważaniem
Zespół CERT Polska | CSIRT NASK
www.cert.pl

UTM a bezpieczeństwo

Dzień dobry

W nawiązaniu do rozmowy telefonicznej z Państwem Opiekunem naszych usług, prosimy o ZAWIESZENIE na okres powiedzmy 1 tygodnia usługi Netia Cloud Firewall. Od czasu, kiedy została aktywowana ta usługa pojawiły się u nas problemy z odbiorem poczty: programy pocztowe odbierają pocztę nieregularnie i często kończą błędem o zerwaniu połączenia. Szukamy przyczyny tych problemów i na początek chcielibyśmy wykluczyć Waszą usługę. Prosimy o informację zwrotną, kiedy byłaby taka możliwość, aby móc diagnozować problem.

Pozdrawiam

Pozdrawiam / Regards / Gruesse

From: [REDACTED]
Sent: Monday, [REDACTED] AM
To: [REDACTED]
Subject: [REDACTED] Wirusy z poczcie

Dzień dobry

Nawiązując do rozmowy z Panem [REDACTED], przesyłam fragment logów z usługi Cloud Firewall. Dziś w ciągu ostatnich 5 minut wykrytych i zablokowanych zostało około 44 połączeń, z uwagi na wykrycie wirusa w poczcie (protokoły POP3 i IMAP). Zdarzeń tego typu jest zdecydowanie więcej i występuje w zasadzie ciągle. Blokada niebezpiecznych połączeń jest poprawnym zachowaniem firewalla.

All FortiGate ▾ Last 5 Minutes [REDACTED]

Source IP: [REDACTED] Add Filter

#	▼ Date/Time	Device ID	Action	Source	Service	Destination IP	Virus/Botnet
1	09:12:59	FG200 [REDACTED]	blocked	[REDACTED]	IMAP	[REDACTED]	W32/BZF!tr
2	09:12:30	FG200 [REDACTED]	blocked	[REDACTED]	IMAP	[REDACTED]	W32/BZF!tr
3	09:12:00	FG200 [REDACTED]	blocked	[REDACTED]	IMAP	[REDACTED]	W32/BZF!tr
4	09:11:31	FG200 [REDACTED]	blocked	[REDACTED]	IMAP	[REDACTED]	W32/BZF!tr
5	09:11:21	FG200 [REDACTED]	blocked	[REDACTED]	POP3	[REDACTED]	



UTM a bezpieczeństwo

From: [REDACTED]
Sent: [REDACTED]
To: [REDACTED]
Cc: Szymkowicz Paweł <Pawel.Szymkowicz@netia.pl>
Subject: [REDACTED] Poprawa zabezpieczeń sieci

Dzień dobry

Nawiązując do rozmowy w sprawie optymalizacji zabezpieczenia sieci LAN i serwerów sugeruję wykonanie kilku, dość czasochłonnych modyfikacji.

Proponuję zmiany zarówno w konfiguracji FortiGate jak również Państwa wewnętrznej infrastruktury LAN.

1. Przegląd przekierowań portów. Aktualnie jest ich około 50. Stanowi to poważną lukę w bezpieczeństwie.

Zalecamy możliwie maksymalne ograniczenie tego typu elementów konfiguracji lub ich całkowite wyłączenie, zmieniając przy tym sposób dostępu do wewnętrznych zasobów poprzez VPN.



UTM a bezpieczeństwo

From: [REDACTED]
Sent: [REDACTED]
To: [REDACTED]
Cc: Szymkowicz Paweł <Pawel.Szymkowicz@netia.pl>
Subject: Rekonfiguracja LAN

Dzień dobry,

Podstawowym zadaniem do wykonania jest segmentacja sieci. Aktualnie Państwa sieci LAN ma płaską strukturę, gdzie wszystkie urządzenia serwery, kamery, komputery są w jednej wspólnej sieci 192.168.11.0/24.

Zalecamy aby podzielić infrastrukturę na kilka segmentów stosując dla nich osobne sieci i VLAN. Do tego celu dodatkowo niezbędny będzie zarządzany przełącznik z obsługą VLAN.

Przykład segmentacji LAN:

LAN Serwery: 10.1.1.0/24

LAN Backup/NAS: 10.2.2.0/24

LAN Kamery: 192.168.8.0/24

LAN Pracownicy: 192.168.10.0/24

LAN Wifi: 192.168.12.0/24

VPN: 10.212.134.0/24

Powyższe niesie za sobą konieczność ustalenia polityk bezpieczeństwa pomiędzy sieciami, tzn. kto i do czego ma mieć dostęp i dla jakich portów/protokołów.



Jakimi usługami zarządzamy?

NETIA
netianext



Netia Cloud Firewall



Netia Managed UTM



Netia Incident Monitoring

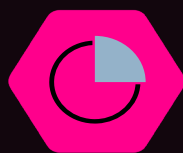
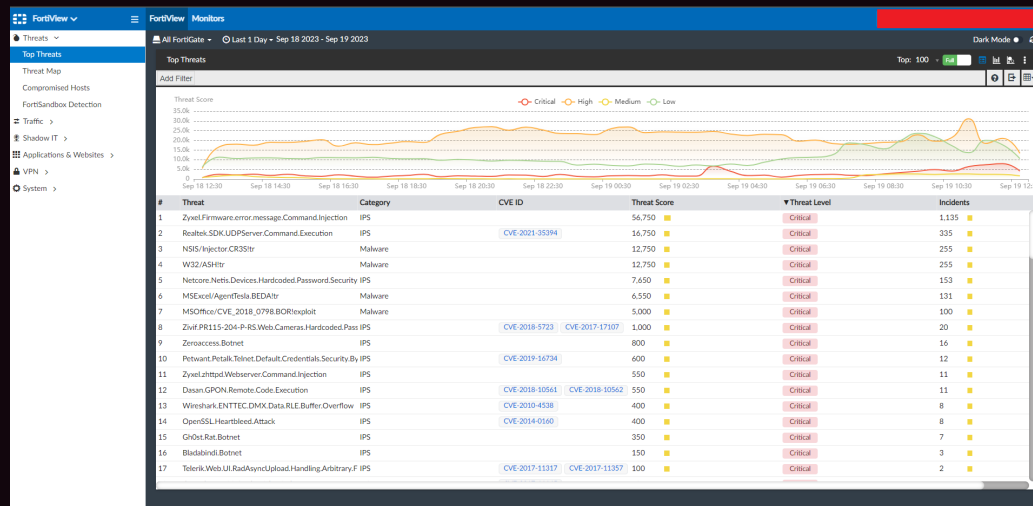


Netia (Secure) SD-WAN+

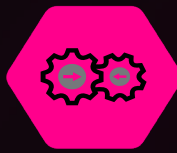


Narzędzia

NETIA
netianext



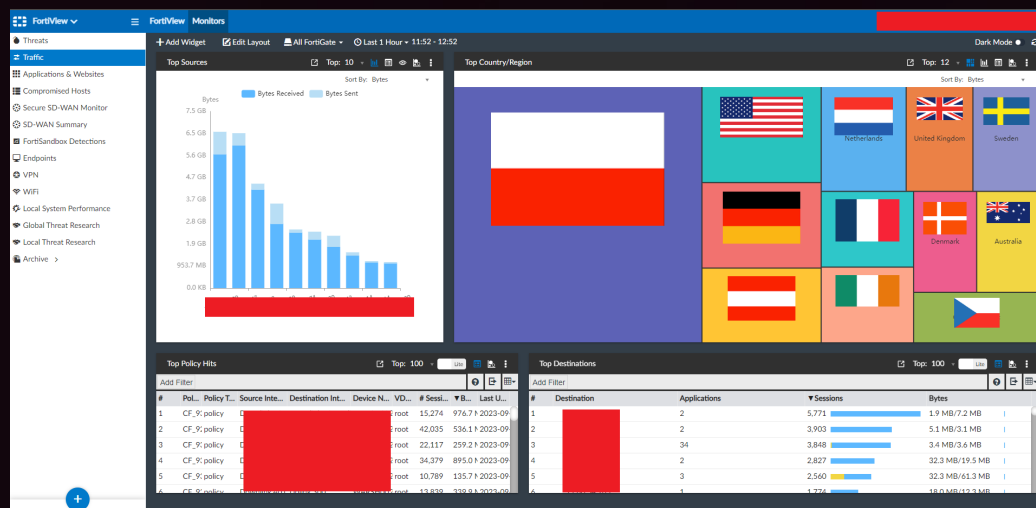
FortiAnalyzer



API



FortiManager



FortiAnalyzer

> FortiSOC

- SOC automation
- Outbreak Alerts
- Incident and Event Management
- Reports



Raporty

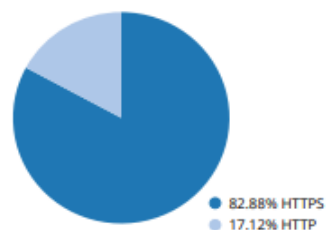
Top 20 Categories By Bandwidth

#	Category
1	Information Technology
2	Streaming Media and Download
3	Business
4	Social Networking
5	Content Servers
6	Search Engines and Portals
7	File Sharing and Storage
8	Internet Radio and TV
9	Advertising
10	Unrated
11	Web-based Email
12	Shopping
13	Reference
14	Web-based Applications
15	Finance and Banking
16	Freeware and Software Downloads
17	Travel
18	Pornography
19	Games
20	News and Media

Botnet Detected

#	Botnet Name
1	RedLine.Stealer.Botnet
2	Mirai.Botnet
3	Bladabindi.Botnet
4	Gh0st.Rat.Botnet
5	SystemBC.Botnet
6	Zeroaccess.Botnet

HTTP SSL Traffic Ratio



Intrusions Detected

#	Attack Name	Severity	CVE-ID
1	Zyxel.Firmware.error.message.Command.Injection	Critical	
2	TrueOnline.ZyXEL.P660HN.V1.Unauthenticated.Command.Injection	Critical	CVE-2017-18368
3	Apache.Log4j.Error.Log.Remote.Code.Execution	Critical	CVE-2021-4104,CVE-2021-44228,CVE-2021-45046
4	Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	Critical	
5	Realtek.SDK.UDP.Server.Command.Execution	Critical	CVE-2021-35394
6	Remote.CMD.Shell	Critical	
7	Bladabindi.Botnet	Critical	
8	Gh0st.Rat.Botnet	Critical	
9	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Critical	CVE-2019-9082,CVE-2018-20062
10	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Critical	CVE-2017-9841

Dziękuję.

Paweł Szymkowicz

Kierownik Działu Utrzymania Usług ICT

FORTINET[®]

 **EXCLUSIVE
NETWORKS**