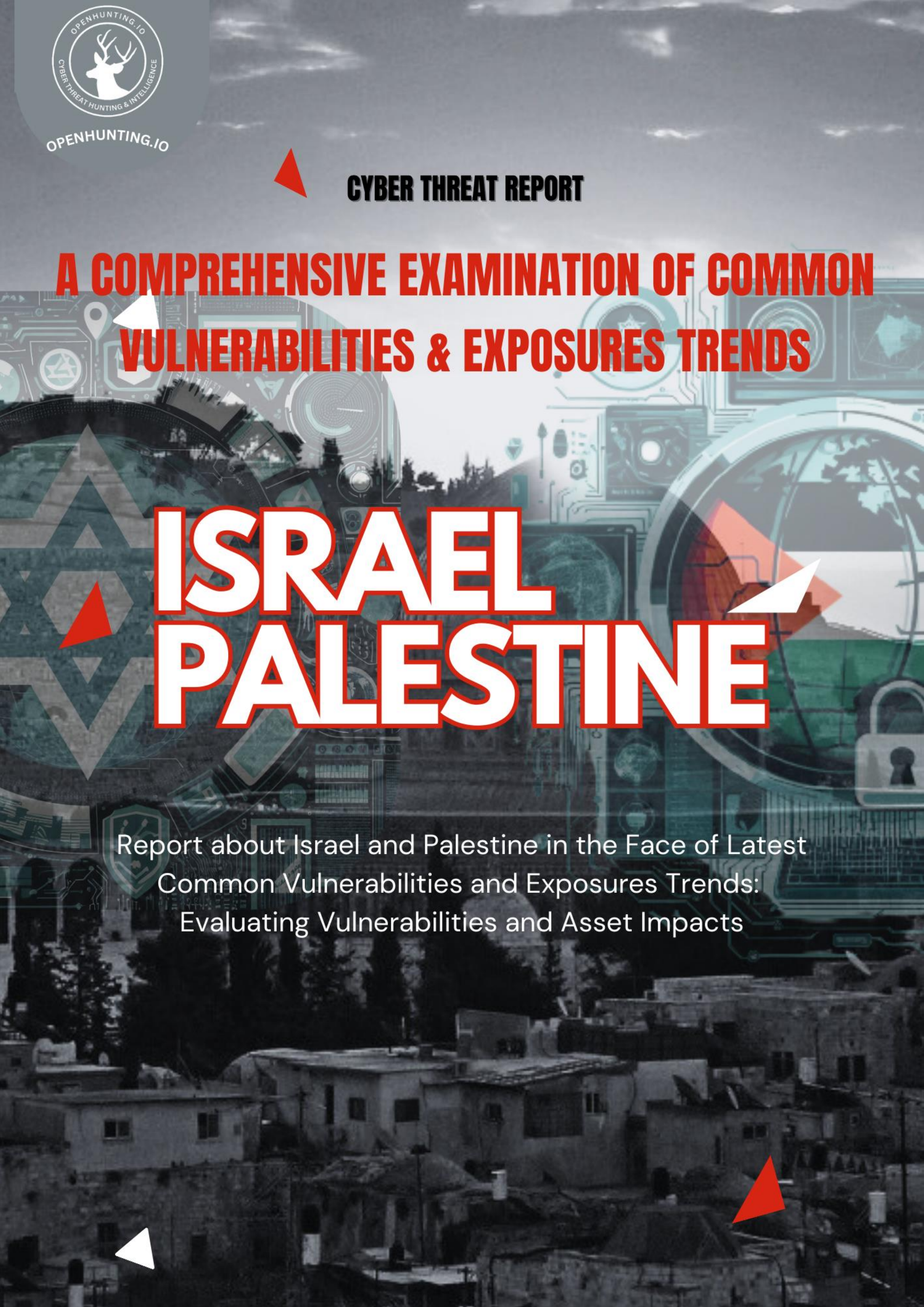
OPENHUNTING.IO



CYBER THREAT REPORT

A COMPREHENSIVE EXAMINATION OF COMMON VULNERABILITIES & EXPOSURES TRENDS

ISRAEL PALESTINE

Report about Israel and Palestine in the Face of Latest Common Vulnerabilities and Exposures Trends: Evaluating Vulnerabilities and Asset Impacts

CYBER THREAT REPORT:
A COMPREHENSIVE EXAMINATION OF COMMON VULNERABILITY & EXPOSURE TRENDS IN ISRAEL PALESTINE

Release Date

Thursday, 16 November 2023

Threat Intelligence Analyst

Rizqy Rionaldy, CTIA, CEH, CHFI, ECIH
Security Researcher @openhunting.io

CONTENTS

INTRODUCTION

The prolonged conflict between Israel and Palestine has not only created tension in the physical realm but has also presented serious challenges in cyberspace. The ongoing war has elicited support and resistance from various parties, including specific stances taken by some countries in responding to the ongoing international conflict.

In this context, cybersecurity has become a profound concern. Coordinated cyber attacks by Advance Persistent Threat (APT) groups operate in a structured and planned manner. APT groups execute attacks with detailed and coordinated methods, leveraging high-level technical expertise to identify and exploit vulnerabilities in the target's cyber infrastructure.

On the other hand, Hacktivist groups operate more openly, utilizing their technical skills as a form of resistance and protest against perceived unjust policies or actions. One notable phenomenon is the occurrence of Web Defacement attacks. In this action, Hacktivists can alter the content, appearance, or functionality of websites by exploiting vulnerabilities in the infrastructure. Although such attacks do not involve data theft or damage to website infrastructure, their impact can be significant on the reputation and trust of website visitors, serving as a means to voice political messages.

In the scenarios of attacks, whether by APT or Hacktivist groups, the role of Common Vulnerability Exposure (CVE) analysis becomes critically important. CVE not only serves as a guide to identify exploitable vulnerabilities but is also actively utilized by parties involved in the conflict to design more effective attacks, exploiting weaknesses that may exist in the target systems.

Threat analysis of the cyber landscape in the Israel-Palestine conflict provides a comprehensive understanding to investigate potential threats that adversaries may exploit. The focus is on vulnerabilities inherent in the infrastructure of both nations. In this context, the role of Common Vulnerability Exposure (CVE) analysis becomes highly significant, offering deep insights into potential vulnerabilities and enabling the identification and in-depth understanding of security risks that can be exploited by parties involved in the conflict.

TOOLS & METHODS

Tools used in this analysis include:

- Shodan (https://www.shodan.io/)
- OSINT

Our method involves inputting keywords related to vulnerabilities into these tools through customized queries, incorporating country codes for both Israel and Palestine. Subsequently, we systematically collect and process the data to ensure meticulous examination and verification of its relevance. This methodological precision enhances our understanding of the cybersecurity landscape during the Israel-Palestine conflict.

UNMASKING VULNERABILITIES: A CLOSER LOOK AT CVES EXPLOITED DURING 2022

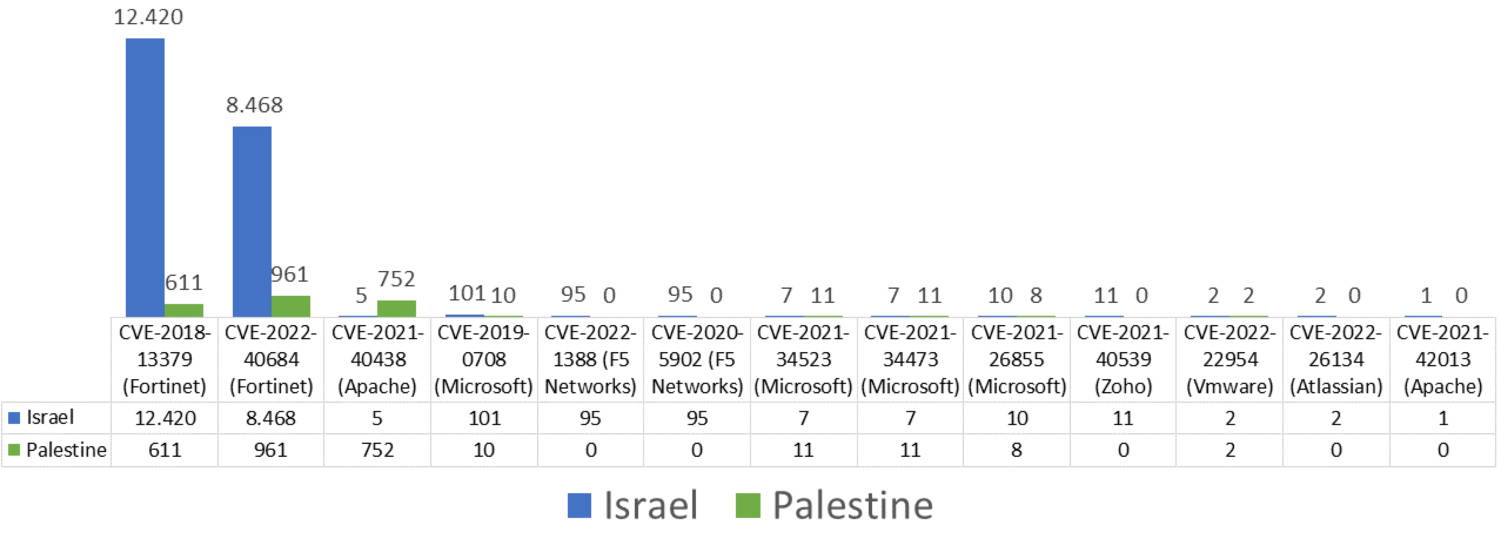
Analysis of potential threats based on Common Vulnerabilities and Exposures (CVE) can be investigated by examining reports related to vulnerabilities recorded in the previous year. On August 3, 2023, the Cybersecurity and Infrastructure Security Agency (CISA) released a detailed document, the "Cyber Security Advisory," discussing vulnerabilities routinely exploited in 2022. The document provides information about CVEs frequently utilized by threat actors. Additionally, it is highlighted that many organizations still use outdated software or system versions that have not been updated, creating a low-risk but significant impact for attackers. This situation raises speculation that such vulnerabilities may be exploited again for future attacks. An analysis was conducted on vulnerability lists, aiming to broaden insights into potential threats.

Apache	Atlassian	Citrix	F5 Networks	Fortinet
CVE-2021- 44228	CVE-2021-26084	CVE-2019-19781	CVE-2022-1388	CVE-2018-13379
CVE-2021-40438	CVE-2022-26134		CVE-2020-5902	CVE-2022-42475
CVE-2021-41773				CVE-2022-40684
CVE-2021-42013				
CVE-2021-45046				

SAP	SonicWALL	Vmware	WSO2	Zimbra
CVE-2022-22536	CVE-2021-20016	CVE-2022-22954	CVE-2022-29464	CVE-2022-24682
	CVE-2021-20021	CVE-2022-22960		CVE-2022-27924
	CVE-2021-20038	CVE-2022-22963		

Ivanti	Microsoft		Oracle	QNAP
CVE-2019-11510	CVE-2021-34473	CVE-2020-1472	CVE-2020-14882	CVE-2022-27593
	CVE-2021-31207	CVE-2021-26855	CVE-2020-14883	
	CVE-2021-34523	CVE-2021-27065		
	CVE-2022-30190	CVE-2021-26858		
	CVE-2017-0199	CVE-2021-26857	**Zoho**	
	CVE-2017-11882	CVE-2022-22047	CVE-2021-40539	
	CVE-2019-0708	CVE-2022-41082		

Following the analysis, a total of 13 potential threat lists were identified, aligning with the assets owned by the observed target. The results of this list were obtained from an analysis of the impacted assets and the threat level. We specifically chose the critical threat level to prioritize the identification of severe vulnerabilities.



	CVE-2018-13379 (Fortinet)	CVE-2022-40684 (Fortinet)	CVE-2021-40438 (Apache)	CVE-2019-0708 (Microsoft)	CVE-2022-1388 (F5 Networks)	CVE-2020-5902 (F5 Networks)	CVE-2021-34523 (Microsoft)	CVE-2021-34473 (Microsoft)	CVE-2021-26855 (Microsoft)	CVE-2021-40539 (Zoho)	CVE-2022-22954 (Vmware)	CVE-2022-26134 (Atlassian)	CVE-2021-42013 (Apache)
■ Israel	12.420	8.468	5	101	95	95	7	7	10	11	2	2	1
■ Palestine	611	961	752	10	0	0	11	11	8	0	2	0	0

According to the queried dataset, an analysis indicates the presence of 13 Common Vulnerabilities and Exposures (CVEs) exhibiting an uneven distribution of potential threats relative to the total assets affected. CVE-2018-13379 and CVE-2022-40684 manifest significantly heightened impact metrics in comparison to other identified vulnerabilities. This provides an understanding that vulnerabilities in Fortinet products continue to have a substantial impact within these two countries.

FUTURE THREAT LANDSCAPE: ANALYZING POTENTIAL EXPLOITS THROUGH CVE TRENDS

The examination of potential threats based on Common Vulnerabilities and Exposures (CVE) can also be explored through an analysis of new CVE trends. By observing news related to recent vulnerabilities, this provides data regarding exploited vulnerabilities. Our focus is on vulnerabilities that could be utilized as an initial access point for attackers, which can be identified through search engine queries.

Adobe	Apache	ArcServe	Asus	Cacti	CasaOS
CVE-2023-29300	CVE-2023-46604 CVE-2023-25690 CVE-2023-37895 CVE-2023-27524	CVE-2023-26258	CVE-2023-39240 CVE-2023-35086	CVE-2023-39361	CVE-2023-37266

Chamilo	Cisco	CloudPanel	Confluence	Draytek Vigor	F5
CVE-2023-34960	CVE-2023-20025 CVE-2023-20214 CVE-2023-20126	CVE-2023-35885	CVE-2023-22515	CVE-2023-33778	CVE-2023-46747

Fortinet	Gibbon school platform	Hewlett Packard Enterprise	Ivanti	Jorani	Lexmark
CVE-2023-33308	CVE-2023-34598	CVE-2023-30908 CVE-2023-39238 CVE-2023-39239	CVE-2023-35082	CVE-2023-26469	CVE-2023-23560

ManageEngine	Mastodon	mlflow	MOVEit	Ms Exchange Server	NodeBB
CVE-2022-47966	CVE-2023-36460	CVE-2023-3765	CVE-2023-34362 CVE-2023-35708 CVE-2023-35036	CVE-2023-36778	CVE-2023-26045

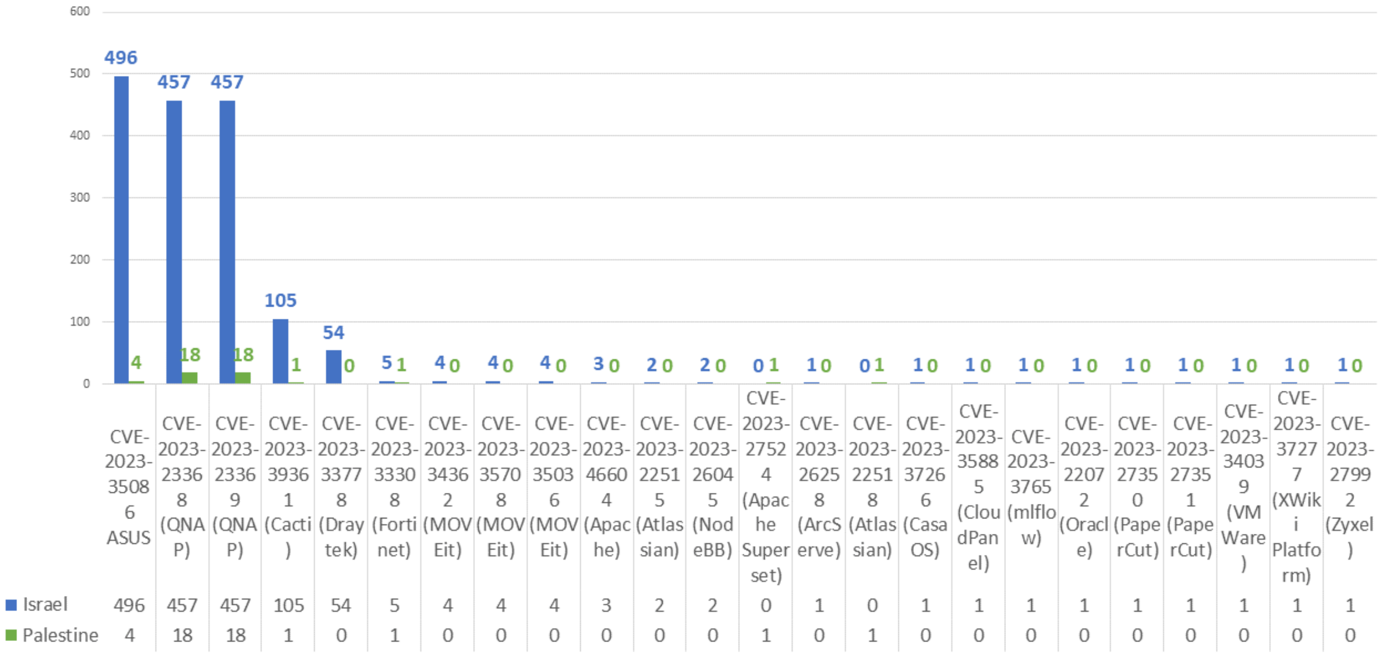
Nuxt.js RCE	OGC Filter SQL Injection	Open-source Memos	OpenTSDB	Oracle	PaperCut MF/NG
CVE-2023-3224	CVE-2023-25157	CVE-2023-4696	CVE-2023-36812 CVE-2023-25826	CVE-2023-22072	CVE-2023-27350 CVE-2023-27351

Pgadmin	QNAP	RaspAP	Seomatic	SharePoint	SolarView
CVE-2023-5002	CVE-2023-23368 CVE-2023-23369	CVE-2022-39986	CVE-2023-41892	CVE-2023-21716	CVE-2023-23333

SPIP	Teamcity	Tsplus	vBulletin	VMWare	Wordpress
CVE-2023-27372	CVE-2023-42793	CVE-2023-31067	CVE-2023-25135	CVE-2023-34039 CVE-2023-34048	CVE-2023-4634 CVE-2023-4596

XWiki Platform	Zyxel
CVE-2023-37277	CVE-2023-28771 CVE-2023-27992 CVE-2023-28771

The list of recent CVE vulnerability trends that we have obtained is subsequently inputted into a search engine to explore their relevance to the observed countries. The result reveals a total of 24 CVEs that have an impact on the assets of both countries under observation.



	CVE-2023-35086 ASUS	CVE-2023-23368 (QNAP)	CVE-2023-23369 (QNAP)	CVE-2023-39361 (Cacti)	CVE-2023-33778 (Draytek)	CVE-2023-33308 (Fortinet)	CVE-2023-34362 (MOVEit)	CVE-2023-35708 (MOVEit)	CVE-2023-35036 (MOVEit)	CVE-2023-46604 (Apache)	CVE-2023-22515 (Atlassian)	CVE-2023-26045 (NodeBB)	CVE-2023-27524 (Apache Superset)	CVE-2023-26258 (ArcServe)	CVE-2023-22518 (Atlassian)	CVE-2023-37266 (CasaOS)	CVE-2023-35885 (CloudPanel)	CVE-2023-3765 (mlflow)	CVE-2023-22072 (Oracle)	CVE-2023-27350 (PaperCut)	CVE-2023-27351 (PaperCut)	CVE-2023-34039 (VMWare)	CVE-2023-37277 (XWiki Platform)	CVE-2023-27992 (Zyxel)
🟦 Israel	496	457	457	105	54	5	4	4	4	3	2	2	0	1	0	1	1	1	1	1	1	1	1	1
🟩 Palestine	4	18	18	1	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0

Based on the search results, it is found that there are five CVEs with the most significant impact on assets in both countries. These vulnerabilities include CVE-2023-58086, CVE-2023-23368, CVE-2023-23369, CVE-2023-39361, and CVE-2023-33778. These vulnerabilities are identified in products from ASUS, QNAP, Cacti, and Draydek.

APT INSIGHTS: CVE EXPLOITATION IN THE CROSSHAIRS OF MIDDLE EAST CYBER THREATS

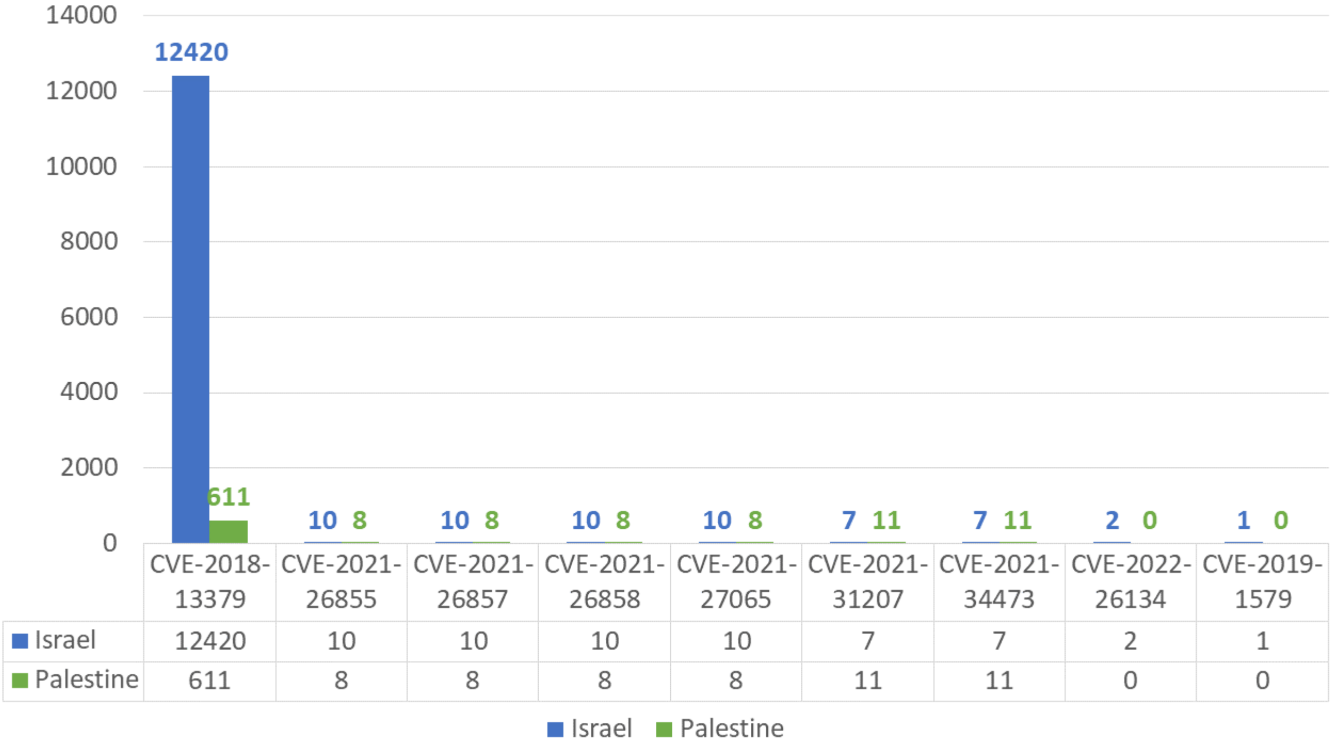
In the final section, the exploration of potential threats based on Common Vulnerabilities and Exposures (CVE) can also be extended through an analysis of Advanced Persistent Threat (APT) data targeting the Middle East.

Subsequently, we conducted a search on Advanced Persistent Threat (APT) activities targeting the Middle East, and then sought to identify the CVEs utilized in these attacks. Following the analysis of the received information, the following is the CVE data based on APTs exploiting vulnerabilities in the Middle East.

DEV-0270	Molerats	POLONIUM	DEV-0133	Sandcat	DEV-0343
CVE-2018-13379 CVE-2021-34473	CVE-2017-0199	CVE-2018-13379	CVE-2019-0604 CVE-2021-26855	CVE-2018-8589 CVE-2019-0797 CVE-2018-8611	CVE-2018-13379 CVE-2021-34473

Storm-1084	APT32	APT33	APT34	APT35	APT39
CVE-2021-44832 CVE-2021-45105 CVE-2021-44832 CVE-2021-45046	CVE-2017-11882 CVE-2016-7255 CVE-2022-42475	CVE-2018-20250 CVE-2017-11774 CVE-2017-0213	CVE-2017-0199 CVE-2017-11882	CVE-2021-34473 CVE-2023-34523 CVE-2021-31207 CVE-2021-44228 CVE-2021-26855 CVE-2021-26857 CVE-2021-26858 CVE-2021-27065 CVE-2018-13379 CVE-2022-47966 CVE-2022-26134	CVE-2022-41128 CVE-2019-11510 CVE-2019-1579 CVE-2018-13379 CVE-2019- 19781

Based on the results of the threat potential exploration, we identified nine CVEs that impact assets in both countries under observation. Presented below are the findings of the search data.

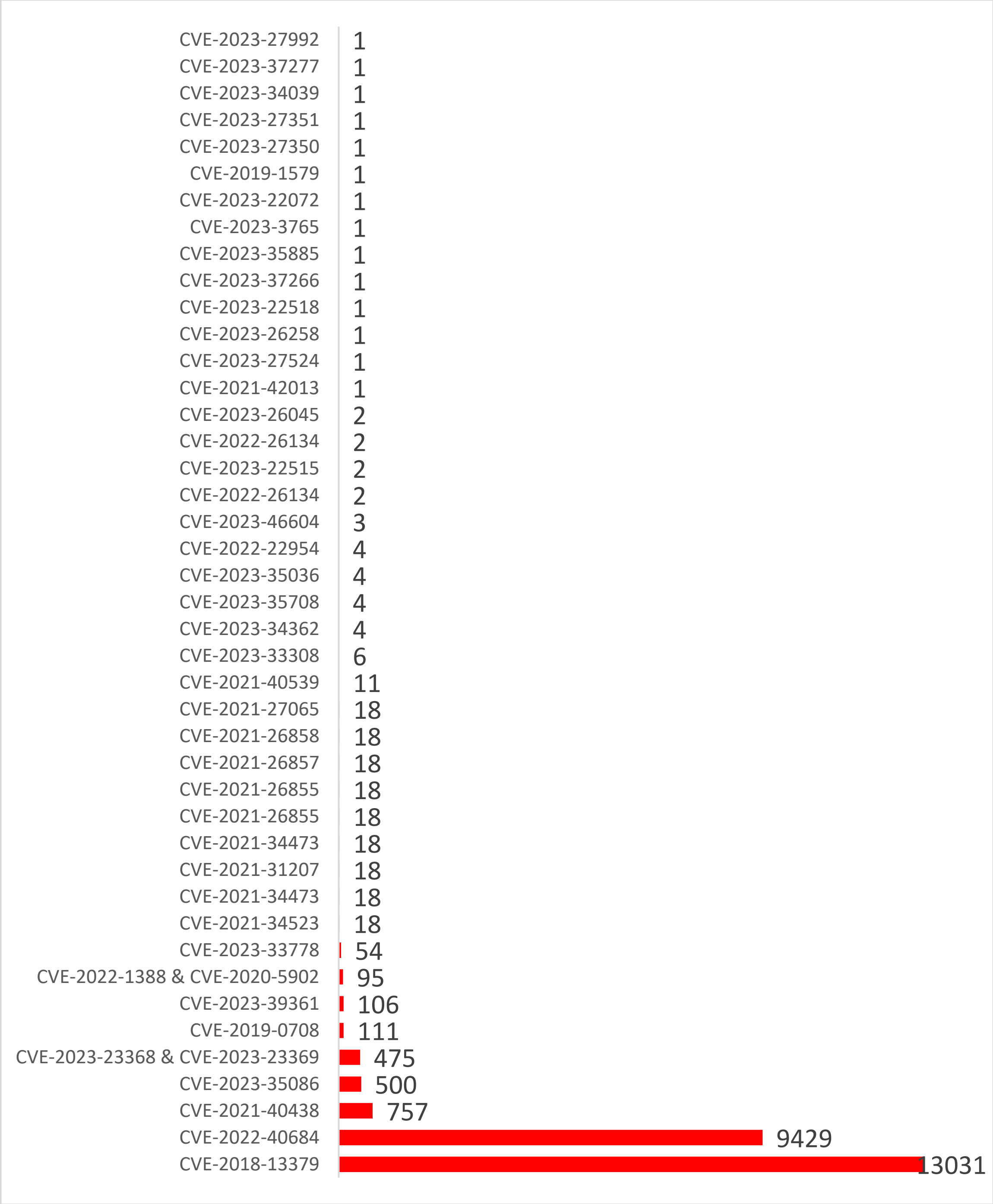


	CVE-2018-13379	CVE-2021-26855	CVE-2021-26857	CVE-2021-26858	CVE-2021-27065	CVE-2021-31207	CVE-2021-34473	CVE-2022-26134	CVE-2019-1579
🟦 Israel	12420	10	10	10	10	7	7	2	1
🟩 Palestine	611	8	8	8	8	11	11	0	0

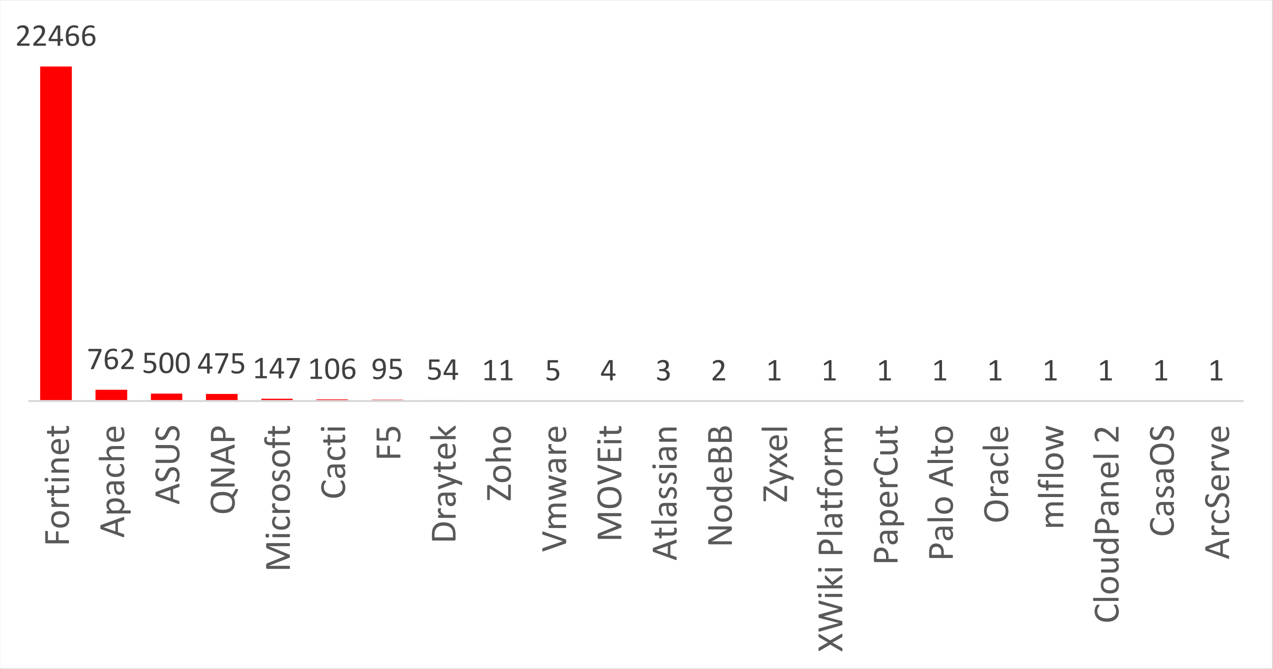
The data results indicate that the most impacted asset is associated with CVE-2018-13379, displaying a significantly higher value compared to other vulnerabilities we identified.

CYBER THREAT CHRONICLES: A HOLISTIC VIEW OF CVE EXPOSURE IN ISRAEL-PALESTINE

we systematically collated the entirety of acquired data predicated on Common Vulnerabilities and Exposures (CVE) recommendations, discernible trends in CVE-centric cyber attacks, and intelligence pertaining to CVEs leveraged by Advanced Persistent Threats (APTs) with a focus on the Middle East.



PRODUCT VULNERABILITY SPOTLIGHT: EXAMINING CVE EXPOSURE ACROSS PLATFORMS



Through the categorization of product names, it is discerned that the product with the highest number of impacted assets is Fortinet, totaling 22,466 hits. Subsequently, others in the ranking include Apache, ASUS, QNAP, and Microsoft.

DECODING THREATS: DELVING INTO THE TOP 10 CVES IMPACTING THE CONFLICT ZONE

In this section, we will provide detailed information regarding the CVEs we have identified, aiming to offer a comprehensive understanding of the vulnerabilities we have uncovered. Our selection of the top 10 is based on the order of the highest number of impacted assets. Moreover, this list is deemed sufficiently illustrative of the potential threats at hand.

1. **CVE-2018-13379**

Description

Vulnerability Type : Path Traversal Vulnerability

CVSS Severity Score	:	**9.8**
Application	:	Fortinet
Severity	:	**Critical**
Affected Product	:	FortiOS

Impact

Total	:	**13.031**
Israel	:	**12.420**
Palestine	:	**611**

Summary

The discovery of a path traversal vulnerability, exemplified by FortiOS vulnerability CVE-2018-13379, poses a significant threat, enabling unauthorized access to restricted files and directories. This flaw affects older versions of Fortinet, FortiOS, and FortiProxy, potentially exposing sensitive information and compromising system security. Notably exploited by APT groups such as DEV-0270, POLONIUM, DEV-0343, APT39, and APT35, this vulnerability has the highest number of affected assets. Urgent patching of vulnerable infrastructure is crucial to mitigate risks and enhance overall system security against potential exploits.

2. CVE-2022-40684

Description

Vulnerability Type	:	Authentication Bypass
CVSS Severity Score	:	**9.8**
Application	:	Fortinet
Severity	:	**Critical**
Affected Product	:	Fortinet FortiOS

Impact

Total	:	**9.429**
Israel	:	**8.468**
Palestine	:	**961**

Summary

CVE-2022-40684 vulnerability not only allows unauthorized access but also empowers adversaries to manipulate user accounts, reroute network traffic, eavesdrop on sensitive data, and download critical system configurations. The potential impact of these malicious activities extends beyond immediate breaches, as the compromised systems may suffer long-term consequences in terms of data integrity, confidentiality, and overall network security. It is imperative for organizations utilizing affected Fortinet products to promptly apply patches and take necessary security measures to mitigate the risks posed by this vulnerability.

3. CVE-2021-40438

Description

Vulnerability Type	:	SSRF (server-side request forgery)
CVSS Severity Score	:	**9.0**
Application	:	Apache
Severity	:	**Critical**
Affected Product	:	Apache HTTP Server 2.4.48 and earlier.

Impact

Total	:	**757**
Israel	:	**5**
Palestine	:	**752**

Summary

CVE-2021-40438 is a critical Server Side Request Forgery (SSRF) vulnerability affecting Apache HTTP Server versions 2.4.48 and earlier. Exploiting this flaw through a specially crafted request URI path could trigger mod_proxy to forward requests to a server chosen by the attacker. SSRF vulnerabilities enable unauthorized requests, bypassing security controls and potentially leading to attacks such as data theft, privilege escalation, and system compromise

4. CVE-2023-35086

Description

Vulnerability Type	:	Remote Arbitrary Code Execution
CVSS Severity Score	:	**9.8**
Application	:	ASUS Router
Severity	:	**Critical**
Affected Product	:	ASUS RT-AX56U V2 & RT-AC86U

Impact

Total	:	**500**
Israel	:	**496**
Palestine	:	**4**

Summary

unauthenticated remote attacker can exploit without privileges to execute arbitrary code, perform system operations, or disrupt services. Affected firmware versions include RT-AX56U V2: 3.0.0.4.386_50460 and RT-AC86U: 3.0.0.4_386_51529. Urgent attention and patching are required to mitigate the risk of remote arbitrary code execution and potential compromise of system integrity.

5. CVE-2023-23368 & CVE-2023-23369

Description

Vulnerability Type	:	Execute Commands via a network
CVSS Severity Score	:	**9.8**
Application	:	QNAP
Severity	:	**Critical**
Affected Product	:	QNAP

Impact

Total	:	**475**
Israel	:	**457**
Palestine	:	**18**

Summary

A critical OS command injection vulnerability has been identified in various versions of QNAP operating systems, posing a significant security risk. Exploitation of this vulnerability could enable remote attackers to execute arbitrary commands via a network connection. To safeguard your device and mitigate this threat, it is strongly advised to consistently update your QNAP system to the latest available version. Regular updates ensure that your NAS (Network Attached Storage) device receives crucial vulnerability fixes and security patches. To determine the latest updates applicable to your specific NAS model, please refer to the product support status. Taking proactive measures by keeping your QNAP operating system up-to-date is essential to maintain the security and integrity of your network-attached storage solution.

6. CVE-2019-0708

Description

Vulnerability Type	:	Remote Code Execution (RCE)
CVSS Severity Score	:	**9.8**
Application	:	Microsoft
Severity	:	**Critical**
Affected Product	:	Exchange Server 2013, 2016 and 2019

Impact

Total	:	**111**
Israel	:	**101**
Palestine	:	**10**

Summary

A critical remote code execution vulnerability in Remote Desktop Services, triggered by unauthenticated attackers sending specially crafted requests via Remote Desktop Protocol, has been identified. Requiring no user interaction, successful exploitation enables arbitrary code execution on the target system, allowing unauthorized activities such as program installation and data manipulation. The security update addresses the flaw by fixing how Remote Desktop Services handles connection requests, emphasizing the immediate need for users and administrators to apply the update to prevent potential system compromise.

7. CVE-2023-39361

Description

Vulnerability Type	:	Unauthenticated SQL Injection
CVSS Severity Score	:	9.8
Application	:	Cacti
Severity	:	**Critical**
Affected Product	:	Cacti

Impact

Total	:	**106**
Israel	:	**105**
Palestine	:	**1**

Summary

Cacti, a widely utilized operational monitoring tool, is currently exposed to a critical SQL injection vulnerability, identified as CVE-2023-39361, with a severity rating of 9.8 on the CVSS scale. This flaw poses a significant risk, potentially enabling an attacker to execute arbitrary code upon successful exploitation. The vulnerability is particularly critical as it allows an unauthenticated user to execute code on a Cacti server, provided a specific data source is chosen for any monitored device. Cacti, known for its network monitoring and graphing capabilities, relies on RRDTool's data storage and graphing functions, offering users a robust and adaptable framework for operational monitoring and fault management. Organizations using Cacti should urgently address this vulnerability to prevent unauthorized code execution and safeguard the integrity of their monitoring systems.

8. CVE-2022-1388 & CVE-2020-5902

Description

Vulnerability Type	:	Missing Authentication Remote Code Execution (RCE)
CVSS Severity Score	:	**9.8**
Application	:	F5
Severity	:	**Critical**
Affected Product	:	F5 Big-IP

Impact

Total	:	**95**
Israel	:	**95**
Palestine	:	**0**

Summary

This vulnerability poses a significant threat, as an unauthenticated attacker with network access to the BIG-IP system via the management port and/or self IP addresses may exploit it to execute arbitrary system commands, create or delete files, and disable services. The risk is particularly concerning as exploitation can occur without the need for authentication, enabling attackers to carry out malicious activities on devices using BIG-IP. The potential consequences include unauthorized command execution, file manipulation, and service disruption. It is crucial for organizations to promptly address and mitigate this vulnerability to prevent unauthorized access and potential compromise of system integrity.

9. CVE-2023-33778

Description

Vulnerability Type	:	Unauthorized Action
CVSS Severity Score	:	**9.8**
Application	:	Draytek
Severity	:	**Critical**
Affected Product	:	Draytek Vigor Routers

Impact

Total	:	**54**
Israel	:	**54**
Palestine	:	**0**

Summary

Draytek Vigor Routers, Access Points, Switches, and Myvigor firmware versions below 3.9.6/4.2.4, v1.4.0, 2.6.7, and 2.3.2, respectively, have been found to employ hardcoded encryption keys. This vulnerability exposes these devices to unauthorized account binding by attackers. Exploiting this flaw enables attackers to associate any affected device with their account, subsequently allowing them to create WCF and DrayDDNS licenses and synchronize them from the website. The use of hardcoded encryption keys poses a serious security risk, compromising the integrity and confidentiality of the affected devices. It is imperative for users to promptly update their firmware to versions 3.9.6/4.2.4 for routers, v1.4.0 for access points, 2.6.7 for switches, and 2.3.2 for Myvigor to mitigate this vulnerability and enhance the security of their Draytek devices.

10. CVE-2021-34523

Description

Vulnerability Type	:	Elevation of Privilege Remote Code Execution (RCE)
CVSS Severity Score	:	**9.8**
Application	:	Microsoft
Severity	:	**Critical**

Affected Product	:	Exchange Server 2013, 2016 and 2019

Impact

Total	:	**18**
Israel	:	**11**
Palestine	:	**7**

Summary

A critical vulnerability impacting Microsoft Exchange Server versions 2013 through 2021 allows unauthorized access and privilege escalation, potentially enabling attackers to assume full control of the server. The exploit involves sending a specially crafted HTTP request to the Exchange Server. This vulnerability has been actively exploited by various threat actors, notably including APT35, emphasizing the urgency for users to apply necessary security patches and safeguards.

CONCLUSION

We have conducted a comprehensive analysis of CVE trends in Israel and Palestine. This analysis encompasses a review of the 2022 CVE History list issued by CISA, trends in CVEs for the year 2023, and a list of CVEs utilized by APT groups targeting the Middle East. Based on our findings, we have identified a total of 43 CVEs impacting assets in Israel and Palestine. Among these findings, it is noteworthy that Fortinet is the product with the highest impact on vulnerability assets. Furthermore, vulnerabilities in this particular device are frequently exploited by attackers targeting countries in the Middle East. Additionally, vulnerabilities in 21 other products have been identified, posing potential risks for exploitation. The outcomes of this observation aim to provide a more comprehensive understanding, reinforcing cybersecurity measures for affected systems.

REFERENCE

https://www.darkowl.com/blog-content/hacktivist-groups-use-defacements-in-the-israel-hamas-conflict/

https://www.cisa.gov/news-events/cybersecurityadvisories/aa23-215a

https://www.hivepro.com/wp-content/uploads/2022/09/Multiple-Iranian-actors-have-launched-attacks-against-the-Albanian-government_TA2022203.pdf

https://www.cyberwarcon.com/the-iranian-evolution

https://www.ic3.gov/media/news/2021/210527.pdf

https://attack.mitre.org/groups/G0059/

OPENHUNTING.IO

Project To Make Threat Hunting and Intelligence Information &

Tools Available for Every One.