



| Flash |

New Exploitation of Existing Vulnerability Announced for Sale

F-2024-09-13a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor, Vulnerability

September 13, 2024

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on September 13, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | New Exploitation of Existing Vulnerability Announced for Sale

› Key Findings

- On September 6, 2024, an actor known as “skng” posted in the dark web forum xss advertising a new malicious script that is allegedly designed to target Fortinet software solutions.
- The product allegedly enables the exploitation of an existing critical vulnerability known as CVE-2022-40684, which was discovered in early October 2022.
- The vast majority of network exploitation leverages old or existing vulnerabilities that have since been remedied by software manufacturers. Threat actors are able to capitalize on the users that have not conducted the appropriate software updates and gain initial network access.

| Details

On September 6, 2024, an actor known as skng posted in the dark web forum xss advertising a new malicious script that is allegedly designed to target Fortinet software solutions. According to skng, the product enables the exploitation of an existing vulnerability known as CVE-2022-40684, which was discovered in early October 2022. Skng is offering the malicious script to two separate buyers only at a cost of USD 3,500

each, which is very likely indicative of attempts to prevent the vulnerability from being identified and mitigated by the software manufacturer or security researchers. Skng further specifies that transactions must use escrow.

- CVE-2022-40684 is an authentication bypass vulnerability with a CVSSv3 score of 9.8 and is classified as “critical.” The vulnerability affects some versions of FortiOS, FortiProxy, and FortiSwitchManager and allows an unauthenticated attacker to perform administrative operations via specially crafted HTTP or HTTPS requests.
- Successfully exploited, CVE-2022-40684 can allow the attacker to gain access to privileged administrative interfaces without being in possession of legitimate credentials. Shortly after the vulnerability’s discovery, mitigating software patches were released alongside customer advisory notices.

The transaction is carried out exclusively through the guarantor and in no other way!

Sale in 2 hands.

Price: 3.5k\$

First contact in PM.

 Complaint

 son of carding

[EXPLOIT] New Fortinet script based on CVE-2022-40684

 snkg ·  Friday at 03:49

AUTOMATIC GUARANTOR CAN BE USED IN THIS TOPIC!

 New deal



snkg

config user ldap

Premium

Registration: 10/30/2022
Messages: 40
Reactions: 18

Friday at 03:49

Price: 3.5k\$
Contacts: P.M.

Approximately 95% of targets from this exploit are not worked out (since they do not have accounts in LDAP).
In this topic I sell a solution that allows you to break into these targets.
All questions and information about the script in PM (only for potential buyers).
After the purchase, you receive full instructions on how to work with the script.

xss post by skng advertising new malicious script

Source: ZeroFox Intelligence

According to the post, approximately 95 percent of the software currently in use cannot be targeted due to users not using lightweight directory access protocol (LDAP) accounts. Skng alleges that the advertised script can remedy this issue, enabling the targeting of a much larger pool of users. It is likely that the malicious script does not enable the targeting of software using up-to-date security patches, but rather, a larger proportion of unpatched systems. If it enabled the targeting of patched software, the price would likely be significantly higher.

- No further detail is provided as to how the script enables exploitation, though the actor promises potential buyers more information and the answers to other questions via private message.

Although skng carries a positive reputation in the xss forum, another well-regarded actor known as “barnaul” commented beneath the post claiming that the script is not useful. Due to the lack of detail provided in the post, the effectiveness of the script cannot be determined.

- Criticizing each other's offerings is very commonly observed in deep and dark web (DDW) forums, even amongst competent and well-regarded actors. There is a likely chance that barnaul's negative response was prompted by a failure to obtain details from skng.



skng
config user ldap
Premium
Registration: 10/30/2022
Messages: 42
Reactions: 18

Monday at 03:09

barnaul said: ↑

Just create an ldap user in the config, lol? And how will it be added to ldap (which may not even exist)?

Hi. There is no point in creating an ldap user, since it will not work anyway. Here is a slightly different solution, if you are interested, I will tell you more in PM.

 Complaint

xss post by barnaul questioning the validity of malicious script

Source: ZeroFox Intelligence

The vast majority of network exploitation leverages old or existing vulnerabilities that have since been remedied by software manufacturers. Threat actors are able to both capitalize on the users that have not conducted the appropriate software updates and leverage malicious DDW services that specialize in uncovering and monetizing new methods of exploiting existing and patched vulnerabilities, such as the script offered by skng.

| Recommendations

- Follow Fortinet-issued guidance on protecting susceptible networks.
 - [hXXps://www.fortiguards.com/psirt/FG-IR-22-377](https://www.fortiguards.com/psirt/FG-IR-22-377)
- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate resources by sensitivity and/or function.
- Implement phishing-resistant multi factor authentication (MFA), secure and complex password policies, and ensure the use of unique and non-repeated credentials.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud-based servers at least once per year—and ideally more frequently.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

| Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

Sources may use **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

Amber

Sources may use **TLP:AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW MAY IT BE SHARED?

Recipients may **NOT** share **TLP:RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Recipients may **ONLY** share **TLP:AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.
Note that **TLP:AMBER+STRICT** restricts sharing to the organization only.

WHEN SHOULD IT BE USED?

Green

Sources may use **TLP:GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

Clear

Sources may use **TLP:CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW MAY IT BE SHARED?

Recipients may share **TLP:GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.

Recipients may share **TLP:CLEAR** information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%