



## | Flash |

# Alleged Sale of Three Exploits, Including Two Zero-Days

F-2024-01-09b

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Vulnerability Exploitation, Deep Dark  
Web & Criminal Underground

**January 9, 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 09:00 AM (EST) on January 9, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

# **| Flash | Alleged Sale of Three Exploits, Including Two Zero-Days**

**> Key Findings**

- On January 7, 2024, untested threat actor “DrakenSnow” announced the sale of three exploits: two zero-day vulnerabilities impacting SonicWall Virtual Private Networks and Microsoft Windows, and a third one-day vulnerability in an undisclosed JetBrains product.
- ZeroFox can neither independently confirm nor disconfirm the veracity of the actor’s claims, as there are an almost equal amount of positive and negative indicators of credibility surrounding the actor and the alleged exploits.
- Despite the typically low credibility of sales of zero-day and one-day exploits, ZeroFox observed their increasing prevalence on deep and dark web (DDW) forums in 2023.

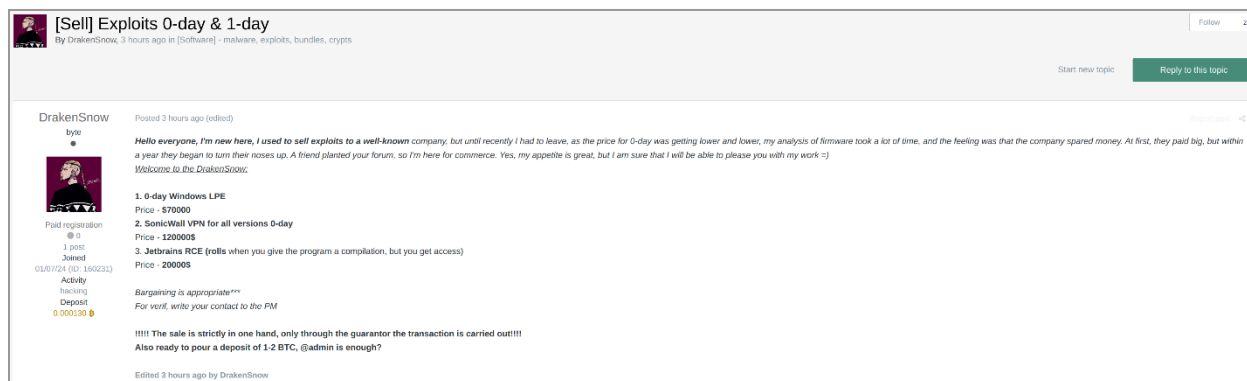
**| Analyst Commentary**

On January 7, 2024, untested Russian-speaking threat actor “DrakenSnow” announced the sale of three exploits on the predominantly Russian-language dark web forum exploit[.]in. The actor claimed to have discovered the exploits on behalf of a well-known

company that discontinued its bug bounty program, which prompted the actor to seek profit within the dark web ecosystem.

The actor's post offers the sale of two zero-day exploits and a third one-day exploit that is likely still working on unpatched systems. The exploits are:

- A SonicWall Virtual Private Network zero-day exploit affecting all versions of the software priced at USD 120,000.
- A Windows Local Privilege Escalation (LPE) zero-day exploit priced at USD 70,000.
- An exploit in an undisclosed JetBrains product priced at USD 20,000. While not explicitly stated, the threat actor implies this is a one-day exploit.



## Translated exploit[.]in post advertising the exploits sale

Source: ZeroFox Intelligence

ZeroFox can neither independently confirm nor disconfirm the veracity of the actor's claims, as there are an almost equal amount of positive and negative indicators of credibility surrounding the actor and the alleged exploits. Despite several positive indicators—including the actor creating a small escrow deposit and agreeing explicitly to conduct all deals via the community escrow—multiple factors indicate the likelihood of a scam. For example:

- An alleged SonicWall zero-day was announced for sale in November 2023 on another forum (RAMP), where the vendor was alleged to be a scammer.
- A Windows LPE has been announced by several different aliases on multiple forums within the last month, indicating that (even if such an exploit is available) it is being resold on the DDW for profit instead of being used to attack systems.

- Legitimate zero-day exploits are typically kept private and used in solitude for as long as possible.

Despite the typically low credibility of sales of zero-day and one-day exploits, ZeroFox observed their increasing prevalence on DDW forums in 2023, indicating scammers likely believe that credibility standards have reduced on the DDW. Historically, such sales have been quickly dismissed as scams. The noticeable absence of negative commentary by forum posters about them and increased prevalence of these types of sales indicates a growing confidence amongst buyers in the legitimacy of zero-day/one-day exploits.

## **| Recommendations**

- Ensure a thorough understanding of your technology stack and patching schedule, as well as those of operating partners.
- Consistently monitor for security patch releases impacting these products and deploy a holistic patch management system to ensure all business IT assets are updated with the latest software as quickly as possible.
- Conduct a thorough assessment of your servers to look for any indicators of compromise (IOCs), and review any relevant activity logs for suspicious behavior.
- Leverage CISA's KEV catalog to prioritize out-of-cycle vulnerability patching.
- Use the ZeroFox Platform's Intelligence Search capability to investigate vulnerabilities and associated exploits.

## | Appendix A: Traffic Light Protocol for Information Dissemination

|                         | Red                                                                                                                                                                                          | Amber                                                                                                                                                                                                                                                                                                                  |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WHEN SHOULD IT BE USED? | Sources may use <b>TLP:RED</b> 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. | Sources may use <b>TLP:AMBER</b> 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 <b>NOT</b> share <b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                              | Recipients may <b>ONLY</b> share <b>TLP:AMBER</b> 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.<br><b>Note that</b> <b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                         | Green                                                                                                                                                                                        | Clear                                                                                                                                                                                                                                                                                                                  |
| WHEN SHOULD IT BE USED? | Sources may use <b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | Sources may use <b>TLP:CLEAR</b> 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 <b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | Recipients may share <b>TLP:CLEAR</b> 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%         |