FLASHPOINT

# Sales and Purchases of Vulnerability Exploits

## 2023 Midyear Report

Vulnerability exploits that were bought, sold, and traded by notable threat actors in the first half of 2023

# Table of Contents

# Introduction

## KNOW YOUR VULNERABILITIES

This report examines the machinations of noteworthy threat actors and illicit marketplaces by examining the exact vulnerability exploits that were listed for sale, purchased, and/or traded in the first half of 2023. The data, research, and analysis featured in this report is derived from Flashpoint's collections and finished intelligence.

To provide readers with deeper context, we have also included several vulnerability classifications and metadata, which can be found in Flashpoint's VulnDB database—including CVSSv2 scores, location, exploit status, and our proprietary ransomware likelihood score.

At the time of publishing, there are over 300,000 documented vulnerabilities—including over 100,000 that cannot be found in CVE and NVD—that affect thousands of vendors and third-party libraries.

All of the vulnerabilities mentioned in this report have been addressed by their respective vendors. If your systems are potentially vulnerable to any of these issues, Flashpoint recommends patching them, as they are constantly attracting threat actor interest and could be used in future exploitation attempts.

# Vulnerability exploits sold in Q1 2023

From January to March 2023, Flashpoint observed mentions of the posted sale, purchase, or trade of exploits for the following vulnerabilities:

| CVE ID | VulnDB ID | Vendor/Product | Exploitation Consequences | Type of Mention |
|---|---|---|---|---|
| CVE-2022-40684 | 302799 | Fortinet/FortiOS | Authentication bypass | Listed for sale—$3,000 |
| CVE-2022-41082 | 302127 | Microsoft/Exchange | Remote code execution | Possible sale—Unknown price |
| CVE-2023-21752 | 309543 | Microsoft/Windows | Local privilege escalation | Listed for sale—$700 |
| CVE-2022-24086 | 282432 | Adobe/Commerce (previously Magento) | Remote code execution | Listed for sale—$30,000 |
| CVE-2022-28672 | 290932 | Foxit/Foxit PDF Reader | Remote code execution | Listed for sale—$1,100 |
| CVE-2023-21608 | 309498 | Adobe/Acrobat | Remote code execution | Listed for sale—$1,100 |
| CVE-2023-21822 | 312482 | Microsoft/Windows | Local privilege escalation | Listed for sale—$8,000 for binary; $13,000 for source code |
| CVE-2022-32548 | 297334 | Draytek/Vigor | Remote code execution | Purchase—Unknown price |
| CVE-2023-23376 | 312429 | Microsoft/Windows | Local privilege escalation | Listed for sale—$6,500 |
| CVE-2023-23415 | 315380 | Microsoft/Windows | Remote code execution | Listed for sale—Unknown price |

*This report features VulnDB's **Ransomware Likelihood score**, which gauges how similar a given vulnerability is to vulnerabilities that are known to have been used in recorded ransomware attacks.*

*A Ransomware Likelihood of "Low" indicates little similarity to known ransomware attacks, while "Critical" indicates extraordinary similarity, or that the given vulnerability has been leveraged in a recorded ransomware attack.*

# Analysis: Q1 2023

### CVE-2022-40684: LISTING OF SALE FOR FORTIOS AUTHENTICATION BYPASS

| | |
|---|---|
| **CVSS (v2)** | 8.3 |
| **Location** | Remote / Network access |
| **Exploit** | Exploit public |
| **Ransomware Likelihood** | **Critical** |

On October 10, 2022, Fortinet released an advisory relating to a fix for a critical vulnerability in FortiOS that could lead to device takeover by a malicious user, escalating to remote code execution. Fortinet informed customers that it was aware of active exploitation of the vulnerability. On March 29, 2023, a threat actor posted for sale a fully realized implementation of the exploit written in Python and Perl for USD $3,000. Flashpoint analysts have not yet observed any posts indicating a successful sale.

### CVE-2022-41082: LISTING OF SALE FOR MICROSOFT EXCHANGE "PROXYNOTSHELL" EXPLOIT

| | |
|---|---|
| **CVSS (v2)** | 9.0 |
| **Location** | Remote / Network access |
| **Exploit** | Exploit public |
| **Ransomware Likelihood** | **Critical** |

The two vulnerabilities, CVE-2022-41040 and CVE-2022-41082 comprise the "ProxyNotShell" vulnerability pair. These zero-day vulnerabilities were disclosed in late September 2022. An attacker could leverage the pair of vulnerabilities to remotely take complete control of an Exchange server.

Flashpoint analysts observed a post on an illicit forum related to CVE-2022-41082. It is unclear whether the poster was selling or sharing an exploit for CVE-2022-41082, as access to the content was gated. However, Flashpoint is including that information here because the exploit has previously been sold—suggesting that interest is ongoing.

**DID YOU KNOW?**

*Half of 2023 Q1's listed or purchased exploits had already been posted last year according to Flashpoint's collections—demonstrating that "older" exploits still garner interest and pose a risk to organizations.*

*The price for an exploit, omitting free exploits, or those whose price was unknown, ranged from USD $700 to $30,000.*

### CVE-2023-21752: LISTING OF SALE FOR MICROSOFT WINDOWS PRIVILEGE ESCALATION EXPLOIT

| | |
|---|---|
| **CVSS (v2)** | 6.6 |
| **Location** | Local access required |
| **Exploit** | Exploit public |
| **Ransomware Likelihood** | Low |

Microsoft released a patch for a local privilege escalation vulnerability, CVE-2023-21752, on January 10, 2023. The vulnerability is caused by an issue in the Windows Backup Service. Flashpoint analysts observed a threat actor selling a functional exploit targeting the vulnerability for USD $500 on January 21, 2023. Three days later, the threat actor increased the price to USD $700.

### CVE-2022-24086: LISTING OF SALE FOR MAGENTO WEB FRAMEWORK EXPLOIT

| | |
|---|---|
| **CVSS (v2)** | 10.0 |
| **Location** | Remote / Network access |
| **Exploit** | Exploit public |
| **Ransomware Likelihood** | Medium |

CVE-2022-24086 was assigned to a vulnerability affecting PHP-based e-commerce platform Magento, which has since been acquired and renamed Adobe Commerce. Originally disclosed on February 13, 2022, the vulnerability may be leveraged remotely to execute arbitrary code without user interactions. At the time of disclosure, Adobe stated that a limited number of Adobe Commerce merchants had been targeted by active exploitation of this vulnerability. It has been reported that it is relatively straightforward to develop functional exploits targeting the vulnerability, but while a number of related GitHub repositories exist publicly, none of them hosts functional exploits or proof-of-concept code targeting this vulnerability.

On February 3, 2023, a threat actor posted a new exploit for sale targeting CVE-2022-24086 along with a Cloudflare web application firewall (WAF) bypass zero-day for USD $30,000. They had previously posted an exploit for this vulnerability back in August 2022.

### CVE-2022-28672 AND CVE-2023-21608: LISTING OF SALE FOR PDF READER RCE EXPLOITS*

| | |
|---|---|
| **CVSS (v2)** | 9.3 |
| **Location** | Context dependent |
| **Exploit** | Exploit public |
| **Ransomware Likelihood** | High |

** Both CVE-2022-28672 and CVE-2023-21608 share the characteristics listed in the chart.*

CVE-2023-21608 and CVE-2022-28672 both identify as use-after-free vulnerabilities affecting various versions of Adobe Reader and Acrobat and Foxit PDF Reader, respectively. Both enable an attacker to remotely execute arbitrary code under the context of the logged-on user. However, exploitation would require some form of user interaction.

POC code is publicly available. Flashpoint analysts observed a threat actor offering functional exploit code for both vulnerabilities on a popular illicit forum on February 11, 2023.

### CVE-2023-21822: PURCHASE OF MICROSOFT WINDOWS PRIVILEGE ESCALATION EXPLOIT

| | |
|---|---|
| **CVSS (v2)** | 7.2 |
| **Location** | Local access required |
| **Exploit** | Exploit unknown |
| **Ransomware Likelihood** | Low |

CVE-2023-21822 is a privilege escalation vulnerability affecting the Microsoft Windows Print Spooler service, and was patched in 2023. By exploiting this vulnerability, an attacker could elevate their privileges, take over the affected device, and execute arbitrary code.

CVE-2023-21822 has not been reported as being exploited in the wild. Flashpoint analysts observed a threat actor selling an exploit targeting CVE-2023-21822 on February 16. The threat actor set the price of the exploit at $8,000 USD for the compiled binary, and USD $13,000 for the source code. Flashpoint observed on March 31 that a notable threat actor displayed interest in purchasing the exploit.

### CVE-2022-32548:
### REQUEST FOR FUNCTIONAL EXPLOIT TARGETING DRAYTEK ROUTERS

| | |
|---|---|
| **CVSS (v2)** | 10.0 |
| **Location** | Remote / Network access |
| **Exploit** | Exploit commercial |
| **Ransomware Likelihood** | High |

CVE-2022-32548 is a vulnerability affecting DrayTek routers that may lead to remote code execution without authentication. While no exploits are publicly available at the time of this writing, a functional exploit is privately held by security firm Trellix, with sufficient technical details publicly available that could aid in the exploit development effort.

In December 2022, Flashpoint observed a threat actor attempting to procure an exploit. Another threat actor responded to this threat in March 2023. However, it is unclear whether any transaction has taken place.

### CVE-2023-23376:
### LISTING OF SALE FOR MICROSOFT WINDOWS PRIVILEGE ESCALATION EXPLOIT

| | |
|---|---|
| **CVSS (v2)** | 7.2 |
| **Location** | Local access required |
| **Exploit** | Exploit public |
| **Ransomware Likelihood** | Low |

The vulnerability CVE-2023-23376 affects various versions of Microsoft Windows. The vulnerability, residing within the Windows Common Log File System Driver, could potentially be leveraged by an attacker with local access to the affected systems to gain the SYSTEM-level privilege context. While no exploits are available publicly at the time of this writing, this vulnerability was actively exploited in the wild at the time of patch release.

On March 6, 2023, Flashpoint observed a threat actor advertising the sale of a functional exploit targeting CVE-2023-23376. The threat actor set the price for the exploit and its accompanying source code for USD $6,500. According to the threat actor, the exploit can be run from a medium-integrity context without triggering Windows Defender, and has a success rate of 90 percent. Flashpoint analysts have observed some threat actor responses, and will continue to monitor the thread for further activities.

## CVE-2023-23415:
## LISTING OF SALE FOR MICROSOFT WINDOWS REMOTE CODE EXECUTION EXPLOIT

| | |
|---|---|
| **CVSS (v2)** | 10.0 |
| **Location** | Remote / Network access |
| **Exploit** | Exploit unknown |
| **Ransomware Likelihood** | Low |

The vulnerability CVE-2023-23415 is caused due to improper handling of certain Internet Control Message Protocol (ICMP) packets. It could potentially be exploited remotely to allow an attacker to execute arbitrary code on affected systems. At the time of publication, Flashpoint is unaware of any functional exploits existing in the public domain.

However, on March 29, a threat actor posted an exploit for CVE-2023-23415 on a popular illicit forum. They are chiefly selling it as a service, but they are also open to the purchase of the source code. No pricing information was provided within the advertisement. At the time of writing, Flashpoint has not observed any responses to the advertisement. However, Flashpoint will continue to monitor the thread for any further activities.

# Vulnerability exploits sold in Q2 2023

From April to June 2023, Flashpoint observed mentions of the sale, purchase, or trade of exploits for the following vulnerabilities:

| CVE ID | VulnDB ID | Vendor/Product | Exploitation Consequences | Type of Mention |
|---|---|---|---|---|
| CVE-2022-32548 | 297334 | Draytek/Vigor | Remote code execution | Purchase—Unknown |
| CVE-2023-27532 | 314497 | Veeam/Backup & Replication | Remote code execution | Listed for sale—Unknown price |
| CVE-2023-32673 | 321026 | HP/Multiple | Local privilege escalation | Listed for sale—Unknown price |
| CVE-2022-31711 | 310612 | VMware/vRealize | Information Disclosure | Listed for sale—Unknown price |
| CVE-2022-41082 | 302127 | Microsoft/Exchange | Remote code execution | Listed for sale—Unknown price |
| CVE-2022-44877 | 309310 | CentOS/Web Panel | Remote code execution | Listed for sale—Unknown price |
| CVE-2023-0669 | 311589 | GoAnywhere/MFT | Remote code execution | Listed for sale—Unknown price |
| CVE-2023-21839 | 310108 | Oracle/WebLogic | Remote code execution | Listed for sale—Unknown price |
| CVE-2023-27350 | 314530 | PaperCut/MF/NG | Remote code execution | Listed for sale—Unknown price |
| CVE-2023-32233 | 320424 | Linux/Kernel | Local privilege escalation | Listed for sale—Unknown price |
| CVE-2022-38005 | 300714 | Microsoft/Windows | Local privilege escalation | Listed for sale—$600 |
| CVE-2023-0386 | 316070 | Linux/Kernel | Local privilege escalation | Listed for sale—Unknown price |
| CVE-2023-2868 | 321988 | Barracuda/Email Security Gateway | Remote code execution | Purchase—$15,000 |
| CVE-2023-24489 | 323584 | Citrix/ShareFile | Remote code execution | Purchase—$25,000 |
| CVE-2023-27363 | 318903 | Foxit/PDF Reader | Remote code execution | Listed for sale—Unknown price |
| CVE-2023-28252 | 317990 | Microsoft/Windows | Local privilege escalation | Listed for sale—Unknown price |
| CVE-2023-29371 | 323480 | Microsoft/Windows | Local privilege escalation | Listed for sale—$10,000 (binary) $15,000 (source) |

# Analysis: Q2 2023

### CVE-2023-0669:
### LISTING OF SALE FOR GOANYWHERE/MFT VULNERABILITY

| | |
|---|---|
| **CVSS (v2)** | 9.3 |
| **Location** | Remote / Network access |
| **Exploit** | Exploit public |
| **Ransomware Likelihood** | **Critical** |

The GoAnywhere/MFT vulnerability was highly leveraged by the ransomware group Clop earlier this year. As of August 9, the total number of victims—those posted on Clop's ransomware clog combined with data from Flashpoint's Cyber Risk Analytics (CRA) platform—totaled more than 650. This number includes companies that were directly attacked by Clop as well as third-party victims.

### CVE-2023-21839:
### LISTING OF SALE FOR ORACLE/WEB LOGIC VULNERABILITIES

| | |
|---|---|
| **CVSS (v2)** | 10.0 |
| **Location** | Remote / Network access |
| **Exploit** | Exploit public |
| **Ransomware Likelihood** | **High** |

The Oracle-Web Logic vulnerabilities had gotten notable attention since exploit code was published by multiple sources. Oracle provided patches on January 17, 2023, with the latest Critical Patch Update. The exploit targets the Listen Port for the Administration Server (TCP/7001). The protocol used with this port is T3—Oracle's proprietary Remote Method Invocation (RMI) protocol.

By binding an instance of the 'weblogic.deployment.jms.ForeignOpaqueReference' class to a named object on the WebLogic Server, attackers can trigger this issue. Using the same technique as in the Log4Shell exploits, the attacker can perform remote code execution.

**DID YOU KNOW?**

*Flashpoint observed 17 vulnerabilities that had mentions associated with the sale, purchase, or trade of an exploit. Of these, two were previously examined in Q1's findings.*

*The price for an exploit in Q2 2023, omitting free exploits, or those whose price was unknown, ranged from USD $600 to $25,000.*

### CVE-2022-38005:
### LISTING OF SALE FOR MICROSOFT WINDOWS LOCAL PRIVILEGE ESCALATION EXPLOIT

| | |
|---|---|
| **CVSS (v2)** | 7.2 |
| **Location** | Local access required |
| **Exploit** | Exploit unknown |
| **Ransomware Likelihood** | Low |

CVE-2022-38005 is a vulnerability in Microsoft Windows Print Spooler. Limited information exists about the details of the vulnerability. A successful local attacker could exploit the vulnerability to potentially gain SYSTEM privileges. Flashpoint analysts observed a threat actor on a popular illicit forum selling an alleged functional exploit targeting this vulnerability. So far, no further comments have been made in the selling thread.

### CVE-2023-2868 AND CVE-2023-24489:
### REQUEST FOR FUNCTIONAL EXPLOITS TARGETING MULTIPLE PRODUCTS

| | |
|---|---|
| **CVSS (v2)** | 10.0 |
| **Location** | Remote / Network access |
| **Exploit** | Exploit public |
| **Ransomware Likelihood** | Medium |

*Data above for CVE-2023-2868*

In two separate threads, the same threat actor solicited for multiple exploits. CVE-2023-2868 is a vulnerability in the Barracuda Email Security Gateway product that could allow an attacker to upload a malicious TAR file to execute arbitrary commands and potentially code.

| | |
|---|---|
| **CVSS (v2)** | 10.0 |
| **Location** | Remote / Network access |
| **Exploit** | Exploit public |
| **Ransomware Likelihood** | High |

*Data above for CVE-2023-24489*

CVE-2023-24489 is a vulnerability in Citrix ShareFile that could allow an attacker to upload a malicious file to execute arbitrary code. In June, Flashpoint observed a soliciting threat actor offering USD $25,000 in the form of XMR or BTC for the Citrix vulnerability exploit. That actor also offered USD $15,000 for the Barracuda exploit.

The Cybersecurity Infrastructure and Security Agency (CISA) added CVE-2023-24489 to the Known Exploited Vulnerabilities Catalog later in August.

## CVE-2023-29371:
## LISTING OF SALE FOR MICROSOFT WINDOWS LOCAL PRIVILEGE ESCALATION

| | |
|---|---|
| **CVSS (v2)** | 7.2 |
| **Location** | Local access required |
| **Exploit** | Exploit unknown |
| **Ransomware Likelihood** | Low |

CVE-2023-29371 is a vulnerability in Microsoft Windows GDI. Limited information exists about the details of the vulnerability. A successful local attacker could exploit the vulnerability to potentially gain SYSTEM privileges. Flashpoint analysts observed a prominent threat actor selling an alleged functional exploit targeting this vulnerability. The selling price is listed at USD $10,000 for a binary and USD $15,000 for the source code

# Combined Intelligence From Flashpoint Ignite and VulnDB

To learn more about how Flashpoint intelligence helps Cyber Threat Intelligence and Vulnerability Management teams solve daily challenges, contact us or sign up for a free trial today.

FREE TRIAL

## ABOUT FLASHPOINT

Trusted by governments, commercial enterprises, and educational institutions worldwide, Flashpoint helps organizations protect their most critical assets, infrastructure, and stakeholders from security risks such as cyber threats, ransomware, vulnerabilities, fraud, and physical threats. Leading security practitioners on physical and corporate security, cyber threat intelligence (CTI), vulnerability management, and vendor risk management teams rely on Flashpoint to proactively identify and mitigate risk and stay ahead of the evolving threat landscape. Learn more at www.flashpoint.io