

HiveForce Labs

# THREAT ADVISORY

**ATTACK REPORT**

## **APT28 Exploits Windows Print Spooler Flaw with GooseEgg**

Date of Publication

April 25, 2024

Admiralty Code

A1

TA Number

TA2024162

# Summary

**Attack Began:** June 2020

**Targeted Regions:** Ukraine, Western Europe, and North America

**Threat Actor:** APT28 (aka Fancy Bear, Forest Blizzard, ATK 5, BlueDelta, Fighting Ursa, FROZENLAKE, Grey-Cloud, Grizzly Steppe, Group 74, Iron Twilight, ITG05, Pawn Storm, Sednit, SIG40, Snakemackerel, Sofacy, Strontium, Swallowtail, TA422, TAG-0700, T-APT-12, TG-4127, Tsar Team, UAC-0028)

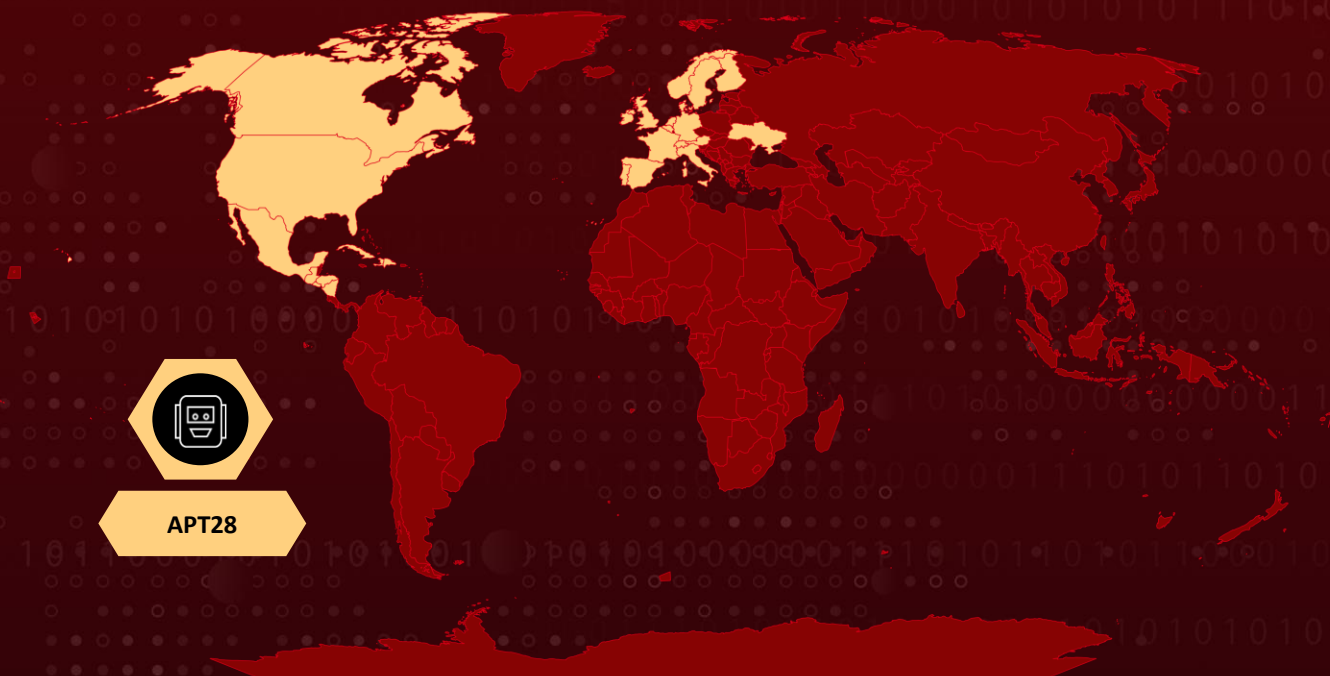
**Malware:** GooseEgg

**Targeted Industries:** Government, NGO, Education, Transportation

**Affected Platform:** Windows




**Attack:** APT28, a Russia-based threat actor, exploited a vulnerability (CVE-2022-38028) in Windows Print Spooler using malware named GooseEgg. This gave them privilege to install additional malware or move laterally within the network to find more sensitive systems. Patching Print Spooler vulnerabilities like CVE-2022-38028 is crucial to mitigate these attacks.

## Attack Regions



Powered by Bing  
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

## CVE

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	MICRO PATCH
CVE-2022-38028	Microsoft Windows Print Spooler Privilege Escalation Vulnerability	Microsoft Windows Print Spooler			

# Attack Details

## #1

A Russia-based threat actor group known as [APT28](#) (also referred to as Forest Blizzard) has been exploiting a vulnerability (CVE-2022-38028) in the Microsoft Windows Print Spooler service. To carry out this exploit, they used custom malware called GooseEgg. This vulnerability allows attackers to escalate privileges on a compromised machine. In simpler terms, it gives them more control over the system than they should have.

## #2

By exploiting this vulnerability, APT28 can achieve two main goals. First, they can install additional malware, such as a backdoor program. Backdoors allow for remote access to a compromised system, enabling attackers to maintain control and potentially steal sensitive information. Second, they can use the vulnerability to move laterally within a network. This means they can jump from one infected machine to another, potentially giving them access to more valuable systems that hold confidential data.

## #3

GooseEgg is a launcher application capable of executing various malicious activities with SYSTEM-level permissions, including remote code execution and lateral movement within compromised networks. The CVE-2022-38028 vulnerability was patched by vendor over a year ago, so the attack is likely targeted. APT groups typically focus their efforts on specific organizations for espionage or intelligence gathering purposes, rather than widespread campaigns.

## #4

This incident also sheds light on a concerning trend. Traditionally, APT groups would invest significant resources into exploiting zero-day vulnerabilities, which are vulnerabilities unknown to software developers and for which there are no patches. However, in this case, APT28 leveraged a publicly known vulnerability. This is because many organizations, unfortunately, do not prioritize patching their systems, leaving them exposed to known exploits.

# #5

The best way to defend against these attacks is to ensure that all systems are up-to-date with the latest security patches. This includes patching the Print Spooler vulnerability (CVE-2022-38028) along with other relevant vulnerabilities like [CVE-2021-34527](#) and [CVE-2021-1675](#) (PrintNightmare). Organizations should prioritize implementing a strong patching strategy to stay ahead of potential threats.

## Recommendations



**Patch Vulnerabilities:** Apply security updates to mitigate vulnerabilities exploited by GooseEgg, such as CVE-2022-38028 for the Print Spooler service. Timely patching reduces the risk of exploitation.



**Disable Print Spooler Service:** Consider disabling the Print Spooler service on domain controllers, especially if it is not required for essential operations. This can reduce the attack surface and minimize the risk of exploitation through this vector.



**Credential Hardening:** Implement measures to harden credentials against theft techniques like LSASS access. This includes enforcing strong password policies and limiting privileged access.



**Endpoint Detection and Response (EDR):** Utilize EDR solutions in block mode to detect and block malicious artifacts associated with GooseEgg. EDR enhances threat detection and response capabilities.



**Implement Attack Surface Reduction:** Employ attack surface reduction rules to prevent common attack techniques used by GooseEgg. These measures can help in blocking credential stealing from critical system components.



## Potential MITRE ATT&CK TTPs

<b><u>TA0001</u></b> Initial Access	<b><u>TA0003</u></b> Persistence	<b><u>TA0004</u></b> Privilege Escalation	<b><u>TA0002</u></b> Execution
<b><u>TA0007</u></b> Discovery	<b><u>TA0042</u></b> Resource Development	<b><u>TA0008</u></b> Lateral Movement	<b><u>TA0005</u></b> Defense Evasion
<b><u>T1112</u></b> Modify Registry	<b><u>T1559.001</u></b> Component Object Model	<b><u>T1559</u></b> Inter-Process Communication	<b><u>T1059</u></b> Command and Scripting Interpreter



<b><u>T1082</u></b> System Information Discovery	<b><u>T1053.005</u></b> Scheduled Task	<b><u>T1053</u></b> Scheduled Task/Job	<b><u>T1588</u></b> Obtain Capabilities
<b><u>T1083</u></b> File and Directory Discovery	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1588.005</u></b> Exploits	<b><u>T1584</u></b> Compromise Infrastructure
<b><u>T1555</u></b> Credentials from Password Stores	<b><u>T1068</u></b> Exploitation for Privilege Escalation	<b><u>T1574.006</u></b> Dynamic Linker Hijacking	<b><u>T1574</u></b> Hijack Execution Flow

## 🔗 Indicators of Compromise (IOCs)

TYPE	VALUE
<b>SHA256</b>	7d51e5cc51c43da5deae5fbc2dce9b85c0656c465bb25ab6bd063a503c1806a9, c60ead92cd376b689d1b4450f2578b36ea0bf64f3963cfa5546279fa4424c2a5, 6b311c0a977d21e772ac4e99762234da852bbf84293386fbe78622a96c0b052f, 41a9784f8787ed86f1e5d20f9895059dac7a030d8d6e426b9ddcaf547c3393aa

## 🔗 Patch Link

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-38028>

## 🔗 References

<https://www.microsoft.com/en-us/security/blog/2024/04/22/analyzing-forest-blizzards-custom-post-compromise-tool-for-exploiting-cve-2022-38028-to-obtain-credentials/>

<https://www.hivepro.com/threat-advisory/russian-threat-actors-leveraging-misconfigured-mfa-to-exploit-printnightmare-vulnerability/>

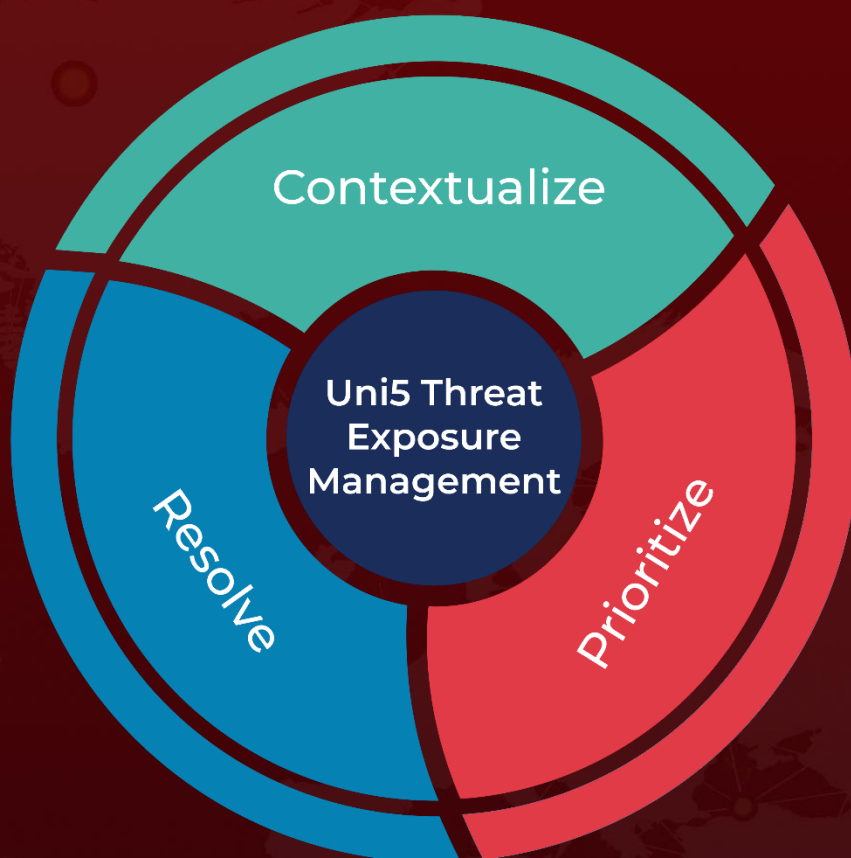
<https://www.hivepro.com/threat-advisory/emergency-patches-have-been-released-by-microsoft-for-printnightmare/>

<https://www.hivepro.com/threat-advisory/apt28s-tactical-exploitation-of-critical-vulnerabilities/>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**April 25, 2024 • 12:30 AM**

© 2024 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)