Threat Signal Report | FortiGuard Labs

Archived: 2026-04-02 11:50:39 UTC

FortiGuard Labs is aware of a report that the Blacktail threat actor exploited the recently patched PaperCut vulnerability (CVE-2023-27350) to distribute the Windows version of Buhti ransomware. The IBM Aspera Faspex code execution vulnerability (CVE-2022-47986) is also being reportedly exploited by the same threat actor.

Why is this Significant?

This is significant because the Blacktail threat actor reportedly exploited the recently patched PaperCut vulnerability to deploy the Windows version of Buhti ransomware. As such the patch should be applied as soon as possible.

What is Buhti Ransomware?

Buhti is a ransomware variant that was first spotted in February 2023 and is designed to encrypt files on compromised machines. Blacktail, a threat actor behind the Buhti ransomware, is believed to use a unique data exfiltration tool to steal various files prior to ransomware deployment. The group demands ransom from victims for file decryption tostop the stolen files from being made available to the public.

Blacktail reportedly exploited the PaperCut MF/NG Improper Access Control vulnerability (CVE-2023-27350) to distribute the Windows version of Buhti ransomware, which is believed to be based on leaked Lockbit 3.0 ransomware code. Another Buhti variant supports Linux platforms and is based on the leaked Babuk ransomware code.

Another report indicates that the Blacktail group also exploited the IBM Aspera Faspex code execution vulnerability (CVE-2022-47986).

What is the PaperCut Vulnerability (CVE-2023-27350)?

CVE-2023-27350 is an authentication bypass vulnerability in PaperCut NG due to improper access control in the vulnerable application. An unauthenticated, remote attacker may be able to exploit this via a crafted request. Successful exploitation could lead to arbitrary code execution within the security context of the affected system.

CISA added CVE-2023-27350 to the Known Exploited Vulnerabilities catalog on April 21st, 2023.

FortiGuard Labs published an Outbreak Alert for the PaperCut vulnerability. Please see the Appendix for a link to "Oubreak Alert: PaperCut MF/NG Improper Access Control Vulnerability".

What is the IBM Aspera Faspex code execution vulnerability (CVE-2022-47986)?

CVE-2022-47986 is a code execution vulnerability in IBM Aspera Faspex stemmed from improper handling of user request. A remote attacker could exploit this vulnerability by sending a crafted message to the target system. Successfully exploiting this vulnerability could result in remote code execution.

CISA added CVE-2022-47986 to the Known Exploited Vulnerabilities catalog on February 21st, 2023.

FortiGuard Labs published Outbreak Alert for the IBM Aspera Faspex code execution vulnerability. Please see the Appendix for a link to "Outbreak Alert: IBM Aspera Faspex Code Execution Vulnerability".

What is the Status of Protection?

FortiGuard Labs has the following AV signatures in place for the known Buhti ransomware samples:

- Linux/Filecoder.BQ!tr
- W32/Lockbit.K!tr.ransom

FortiGuard Labs has the following IPS signatures in place for CVE-2023-27350 and CVE-2022-47986 respectively:

- PaperCut.NG.SetupCompleted.Authentication.Bypass
- IBM.Aspera.Faspex.CVE-2022-47986.Remote.Code.Execution

Outbreak Alert

IBM Aspera Faspex could allow a remote attacker to execute code on the system, caused by a YAML deserialization flaw. By sending a specially crafted obsolete API call, an attacker could exploit this vulnerability to execute arbitrary code on the system.

CVE-2023-27350 allows for an unauthenticated attacker to execute Remote Code Execution (RCE) on a PaperCut Application Server. Vulnerability exists within the SetupCompleted class and according to the vendor, this could be achieved remotely and without the need to log in.

View the full Outbreak Alert Report
