Apache ActiveMQ Vulnerability (CVE-2023-46604)

Security Advisory Summary

Threat actors are taking advantage of insecure deserialization in Apache ActiveMQ, which allows them to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause the broker to instantiate any class on the classpath. Proof-of-concept (POC) exploit code and vulnerability details are both publicly available. This vulnerability is currently being exploited by attackers, who are trying to use this vulnerability to deploy ransomware but have been unsuccessful. The Apache ActiveMQ vulnerability is being tracked as CVE-2023-46604 with a CVSS score of 10.0 and was disclosed on October 27, 2023.

What happened?

This vulnerability has been reported as exploited in the wild to public facing servers.

Advisory Details

Severity

10.0 Critical

Advisory ID

CVE-2023-46604

First Published

10/27/2023

Last Updated

10/28/2023

CVSS Score

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:H

Have there been any reports?

We have not received any reports from our customers of attacks related to this vulnerability.

How is SolarWinds addressing this?

For SolarWinds products Database Performance Analyzer (DPA) prior to 2023.4 and Web Help Desk (WHD), Apache ActiveMQ is enabled under the default setting, which allows only local connections and does not accept remote connections.

What actions should I take?

SolarWinds recommends blocking port 61616 in your firewall in an abundance of caution for both DPA prior to 2023.4 and WHD.