

Explore how attackers operate and their favorite tools and targets in our new SANS research. [Get the Report](#)



FOX

[BLOG](#) // [ADVISORIES](#) // [JUL 13, 2022](#)

Netwrix Auditor Advisory

By: Jordan Parkin, Senior Security Consultant



This site uses cookies to provide you with a great user experience. By continuing to use our website, you consent to the use of cookies. To find out more about the cookies we use, please see our [Privacy Policy](#).

Accept

ADVISORY SUMMARY

The following document describes identified vulnerabilities in the Netwrix Auditor application in supported versions prior to 10.5.

Product Vendor

Netwrix

Product Description

Auditor is IT auditing software used to track assets within an organization. The product's official website is <https://www.netwrix.com/auditor.html>. The latest version of the application is 10.5, released on June 6, 2022.

Vulnerabilities List

1 vulnerability was identified within the Netwrix Auditor application:

Insecure Object Deserialization

These vulnerabilities are described in the following sections.

Affected Version

All supported versions prior to 10.5

Summary of Findings

The Netwrix Auditor application is affected by an insecure object deserialization issue that allows an attacker to execute arbitrary code with the privileges of the affected service. This issue is caused by an unsecured .NET remote port accessible on TCP port 8004.

This site uses cookies to provide you with a great user experience. By continuing to use our website, you consent to the use of cookies. To find out more about the cookies we use, please see our [Privacy Policy](#).

Accept

Solution

Update to version 10.5

Insecure Object Deserialization

Netwrix Auditor is vulnerable to an insecure object deserialization issue that is caused by an unsecured .NET remoting service. An attacker can submit arbitrary objects to the application through this service to achieve remote code execution on Netwrix Auditor servers.

Vulnerability Details

CVE ID: *Pending*

Vulnerability Type: Insecure Object Deserialization

Access Vector: ☒ Remote, ☐ Local, ☐ Physical, ☐ Context dependent, ☐ Other (if other, please specify)

Impact: ☒ Code execution, ☐ Denial of service, ☒ Escalation of privileges, ☐ Information disclosure, ☐ Other (if other, please specify)

Security Risk: ☒ Critical, ☐ High, ☐ Medium, ☐ Low

Vulnerability: CWE-502

The Netwrix Auditor application is affected by an insecure object deserialization issue that allows an attacker to execute arbitrary code with the privileges of the affected service. In a typical real-world scenario, Netwrix Auditor services would be running with a highly privileged account, which could lead to full compromise of the Active Directory environment.

This issue was discovered by performing a TCP port scan of a Netwrix

This site uses cookies to provide you with a great user experience. By continuing to use our website, you consent to the use of cookies. To find out more about the cookies we use, please see our [Privacy Policy](#).

Accept

Accept

FIGURE 5 – Code executed through the .NET remoting service

Since the command was executed with **NT AUTHORITY\system** privileges, exploiting this issue would allow an attacker to fully compromise the Netwrix server.

SUBSCRIBE TO BISHOP FOX'S SECURITY BLOG

Be first to learn about latest tools,
advisories, and findings.

Email Address:

Submit



This site uses cookies to provide you with a great user experience. By continuing to use our website, you consent to the use of cookies. To find out more about the cookies we use, please see our [Privacy Policy](#).

Accept

has worked for Fortune 500 companies across a wide range of industries, including finance, healthcare, technology, and manufacturing.

[More by Jordan](#)

RECOMMENDED POSTS

You might be interested in these related posts.



Nov 21, 2022

Log HTTP Requests, Version 1.3.1, Advisory

This site uses cookies to provide you with a great user experience. By continuing to use our website, you consent to the use of cookies. To find out more about the cookies we use, please see our [Privacy Policy](#).

[Accept](#)



Jun 23, 2022

FileStack Upload Advisory



May 10, 2022

CVE-2022-1388: Scan BIG-IP for Exact Release Versions

Cosmos Platform

Platform Overview

This site uses cookies to provide you with a great user experience. By continuing to use our website, you consent to the use of cookies. To find out more about the cookies we use, please see our [Privacy Policy](#).

Accept

Application Security

Cloud Security

IoT & Product Security

Network Security

Red Team & Readiness

Google, Facebook, & Amazon Partner Assessments

Resources

Resource Center

Blog

Advisories

Tools

Our Customers

Partners

Partner Programs

Partner Directory

Become a Partner

Company

About Us

Careers We're Hiring

Events

This site uses cookies to provide you with a great user experience. By continuing to use our website, you consent to the use of cookies. To find out more about the cookies we use, please see our [Privacy Policy](#).

Accept

Copyright © 2022 Bishop Fox

[Privacy Statement](#)

[Responsible Disclosure Policy](#)

This site uses cookies to provide you with a great user experience. By continuing to use our website, you consent to the use of cookies. To find out more about the cookies we use, please see our [Privacy Policy](#).

Accept