



NextGen Healthcare Mirth Connect Deserialization of Untrusted Data Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2023-43208
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-26 17:15:00 UTC
Updated	2024-01-31 18:15:00 UTC
Description	NextGen Healthcare Mirth Connect before version 4.4.1 is vulnerable to unauthenticated remote code execution. Note that

Risk And Classification

EPSS: 0.944160000 probability, percentile 0.999800000 (date 2026-04-01)

CISA KEV: Listed on 2024-05-20; due 2024-06-10; ransomware use Known

Problem Types: NVD-CWE-noinfo

CISA Known Exploited Vulnerability

Vendor	NextGen Healthcare
Product	Mirth Connect
Name	NextGen Healthcare Mirth Connect Deserialization of Untrusted Data Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. Please check with specific vendors for information on patching status. For more information, please see: https://github.com/nextgenhealthcare/connect/wiki/4.4.1---What%27s-New ; https://nvd.nist.gov/vuln/detail/CVE-2023-43208

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nextgen	Mirth Connect	All	All	All	All

References

Reference	Source	Link	Ta
Mirth Connect 4.4.0 Remote Command Execution ≈ Packet Storm		packetstormsecurity.com	

NextGen Mirth Connect Remote Code Execution Vulnerability (CVE-2023-43208) – Horizon3.ai	MISC	www.horizon3.ai	
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[730974](#) NextGen Mirth Connect Java XStream Remote Code Execution (RCE) Vulnerability

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report