

CVE-2023-43208

NextGen Healthcare Mirth Connect Deserialization of Untrusted Data Vulnerability

Exigent CISA KEV since May 20, 2024 Actively exploited Ransomware use known Public exploit module (Metasploit)

NextGen Healthcare Mirth Connect before version 4.4.1 is vulnerable to unauthenticated remote code execution. Note that this vulnerability is caused by the incomplete patch of CVE-2023-37679.

EVRS 89 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.827 99.67th percentile · FIRST	CISA DEADLINE Jun 10, 2024 KEV since 2024 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score
 ☐ not counted
 evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.827 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. **CISA note:** 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.
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
mirth connect	< 4.4.1	4.4.1	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-pj5c-qr29-6746	github.com	github.com/nextgenhealthcare/connect/wiki/4.4.1---What%27s-New
NVD	nvd.nist.gov/vuln/detail/CVE-2023-43208	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-47627	Current data	evulnable.com/vulnerability-management/cve/CVE-2023-43208

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.