



CVE-2023-37679

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

Summary

CVE	CVE-2023-37679
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-03 03:15:00 UTC
Updated	2024-01-31 18:15:00 UTC
Description	A remote command execution (RCE) vulnerability in NextGen Mirth Connect v4.3.0 allows attackers to execute arbitrary co

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nextgen	Mirth Connect	4.3.0	All	All	All

References

Reference	Source	Link	Tags
Mirth Connect 4.4.0 Remote Command Execution ~ Packet Storm		packetstormsecurity.com	
Healthcare Integration Engine Mirth® Connect by NextGen Healthcare	MISC	mirth.com	
Mirth Connect	MISC	www.ihteam.net	
Award-winning EHR/EMR software NextGen Healthcare	MISC	nextgen.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

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