



CVE-2023-0296

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

Summary

CVE	CVE-2023-0296
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-17 21:15:00 UTC
Updated	2023-02-13 04:53:00 UTC
Description	The Birthday attack against 64-bit block ciphers flaw (CVE-2016-2183) was reported for the health checks port (9979) on et

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Openshift	4.11	All	All	All

References

Reference	Source
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
2161287 – (CVE-2023-0296) CVE-2023-0296 openshift: etcd grpc-proxy vulnerable to The Birthday attack against 64-bit block cipher	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
CVE Program record	CVE.O
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [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](#)