



CVE-2018-3973

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2018-3973
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-02-06 21:29:00 UTC
Updated	2023-02-03 17:58:00 UTC
Description	An exploitable out of bounds write exists in the CAL parsing functionality of Canvas Draw version 5.0.0. A specially crafted

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Canvasgfx	Canvas Draw	5.0.0	All	All	All
Application	Canvasgfx	Canvas Draw	5.0.0	All	All	All

References

Reference	Source	Link	Ta
ACD Systems Canvas Draw Multiple Out of Bounds Write Remote Code Execution Vulnerabilities	BID	www.securityfocus.com	Th
TALOS-2018-0638 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	talosintelligence.com	Ex
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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

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