



CVE-2020-14979

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

Summary

CVE	CVE-2020-14979
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-11 18:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	The WinRing0.sys and WinRing0x64.sys drivers 1.2.0 in EVGA Precision X1 through 1.0.6 allow local users, including low i

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Evga	Precision X1	All	All	All	All
Application	Winring0 Project	Winring0	1.2.0	All	All	All
Application	Winring0 Project	Winring0	1.2.0	All	All	All

References

Reference	Source	Link
EVGA - Software - EVGA Precision X1™	MISC	www.evga.com
CVE-2020-14979: Local Privilege Escalation in EVGA Precision X1 by Matt Hand Posts By SpecterOps Team Members	MISC	posts.specterops.io
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[376704](#) EVGA Precision X1 Local Privilege Escalation Vulnerability

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)