

CVE-2015-2291

Intel Ethernet Diagnostics Driver for Windows Denial-of-Service Vulnerability

CISA KEV since Feb 10, 2023

Actively exploited

Ransomware use known

(1) IQVW32.sys before 1.3.1.0 and (2) IQVW64.sys before 1.3.1.0 in the Intel Ethernet diagnostics driver for Windows allows local users to cause a denial of service or possibly execute arbitrary code with kernel privileges via a crafted (a) 0x80862013, (b) 0x8086200B, (c) 0x8086200F, or (d) 0x80862007 IOCTL call.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.090 95.3rd percentile · FIRST	CISA DEADLINE Mar 3, 2023 KEV since 2023 · 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	0.090 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
ethernet diagnostics driver iqvw32.sys	1.03.0.7	no fixed version listed	NVD
ethernet diagnostics driver iqvw64.sys	1.03.0.7	no fixed version listed	NVD
windows	—	no fixed version listed	NVD

Sources

Vendor guidance [security-center.intel.com/advisory.aspx?](https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00051&languageid=en-fr)[intelid=INTEL-SA-00051&languageid=en-fr](https://nvd.nist.gov/vuln/detail/CVE-2015-2291)**NVD** nvd.nist.gov/vuln/detail/CVE-2015-2291**ENISA EUVD** [euvd.enisa.europa.eu/vulnerability/](https://euvd.enisa.europa.eu/vulnerability/EUVD-2015-2389)
[EUVD-2015-2389](https://euvd.enisa.europa.eu/vulnerability/EUVD-2015-2389)**intel.com** [intel.com/content/www/us/en/security-center/](https://intel.com/content/www/us/en/security-center/advisory/intel-sa-00051.html)
[advisory/intel-sa-00051.html](https://intel.com/content/www/us/en/security-center/advisory/intel-sa-00051.html)**CISA KEV** cisa.gov/known-exploited-vulnerabilities-catalog**Current data** [evulnable.com/vulnerability-management/cve/](https://evulnable.com/vulnerability-management/cve/CVE-2015-2291)
[CVE-2015-2291](https://evulnable.com/vulnerability-management/cve/CVE-2015-2291)

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