

CVE-2018-19323

GIGABYTE Multiple Products Privilege Escalation Vulnerability

Exigent

CISA KEV since Oct 24, 2022

Actively exploited

Ransomware use known

The GDrv low-level driver in GIGABYTE APP Center v1.05.21 and earlier, AORUS GRAPHICS ENGINE before 1.57, XTREME GAMING ENGINE before 1.26, and OC GURU II v2.08 exposes functionality to read and write Machine Specific Registers (MSRs).

EVRS 85/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.084 95th percentile · FIRST	CISA DEADLINE Nov 14, 2022 KEV since 2022 · 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	0.084 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent 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
aorus graphics engine	< 1.57	1.57	NVD
gigabyte app center	≤ 1.05.21	after 1.05.21	NVD
oc guru ii	2.08	no fixed version listed	NVD
xtreme gaming engine	< 1.26	1.26	NVD

Sources

Vendor guidance github.com/advisories/GHSA-237x-ggjj9-vvhf
NVD nvd.nist.gov/vuln/detail/CVE-2018-19323

Additional guidance gigabyte.com/Support/Security/1801
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2018-11021

Current data evulnable.com/vulnerability-management/cve/CVE-2018-19323

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