

CVE-2018-19322

GIGABYTE Multiple Products Code Execution Vulnerability

CISA KEV since Oct 24, 2022

Actively exploited

Ransomware use known

The GPCIDrv and GDrv low-level drivers 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 expose functionality to read/write data from/to IO ports. This could be leveraged in a number of ways to ultimately run code with elevated privileges.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.018 78.5th 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	0.018 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
aorus graphics engine	< 1.57	1.57	NVD
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-vv86-whxx-rv84
NVD nvd.nist.gov/vuln/detail/CVE-2018-19322

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2018-11020

Current data evulnable.com/vulnerability-management/cve/CVE-2018-19322

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