

CVE-2020-15999

Google Chrome FreeType Heap Buffer Overflow Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Heap buffer overflow in FreeType in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

EVRS 77 / ₁₀₀ Urgent priority	CVSS V3.1 9.6 Critical · NVD	EPSS 0.639 99.22nd percentile · FIRST	CISA DEADLINE Nov 17, 2021 KEV since 2021 · 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	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.639 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.6	☐ 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
chrome	< 86.0.4240.111	no fixed version listed	NVD
freetype	≥ 2.6.0 < 2.10.4	no fixed version listed	NVD
backports sle	15.0	no fixed version listed	NVD
ontap select deploy administration utility	—	no fixed version listed	NVD
debian linux	10.0	no fixed version listed	NVD
fedora	31	no fixed version listed	NVD

Sources

Vendor guidance	lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/J3QVIGAAJ4D62YEJAJJWMCCBCOQ6TVL7/	NVD	nvd.nist.gov/vuln/detail/CVE-2020-15999
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2020-1435
Current data	evulnable.com/vulnerability-management/cve/CVE-2020-15999		

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