CVE-2020-0601

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-0601
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-14 23:15:00 UTC
Updated	2022-08-12 18:40:00 UTC
Description	A spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) cert

Risk And Classification

EPSS: 0.940930000 probability, percentile 0.999050000 (date 2026-04-01)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

Problem Types: CWE-295

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Windows
Name	Microsoft Windows CryptoAPI Spoofing Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	Reference CISA's ED 20-02 (https://www.cisa.gov/news-events/directives/ed-20-02-mitigate-windows-vulnerabilities-january-2020-patch-tuesday) for further guidance and requirements. Note: The due date for addressing this vulnerability aligns with the requirements outlined in ED 20-02. https://nvd.nist.gov/vuln/detail/CVE-2020-0601

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Golang	Go	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 10	1709	All	All	All
Operating System	Microsoft	Windows 10	1803	All	All	All

Operating System	Microsoft	Windows 10	1809	All	All	All
Operating System	Microsoft	Windows 10	1903	All	All	All
Operating System	Microsoft	Windows 10	1909	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 10	1709	All	All	All
Operating System	Microsoft	Windows 10	1803	All	All	All
Operating System	Microsoft	Windows 10	1809	All	All	All
Operating System	Microsoft	Windows 10	1903	All	All	All
Operating System	Microsoft	Windows 10	1909	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	1803	All	All	All
Operating System	Microsoft	Windows Server 2016	1903	All	All	All
Operating System	Microsoft	Windows Server 2016	1909	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	1803	All	All	All
Operating System	Microsoft	Windows Server 2016	1903	All	All	All
Operating System	Microsoft	Windows Server 2016	1909	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All

References

Reference	Source	Link	Tags
CurveBall Microsoft Windows CryptoAPI Spoofing Proof Of Concept ≈ Packet Storm	MISC	packetstormsecurity.com	
CurveBall Microsoft Windows CryptoAPI Spoofing Proof Of Concept ≈ Packet Storm	MISC	packetstormsecurity.com	
N/A	N/A	portal.msrc.microsoft.com	Patch, Vendo
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500857 Alpine Linux Security Update for containerd

504639 Alpine Linux Security Update for containerd

672362 EulerOS Security Update for golang (EulerOS-SA-2022-2766)

672365 EulerOS Security Update for golang (EulerOS-SA-2022-2731)