



# KNOWN EXPLOITED VULNERABILITIES CATALOG

[Download CSV version](#)

[Download JSON version](#)

[Download JSON schema](#)

[Subscribe to the Known Exploited Vulnerabilities Catalog Update Bulletin](#)

[Back to previous page for background on known exploited vulnerabilities](#)

Show  entries

Search:

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
CVE-2022-29499	Mitel	MiVoice Connect	Mitel MiVoice Connect Data Validation Vulnerability	2022-06-27	The Service Appliance component in Mitel MiVoice Connect allows remote code execution due to incorrect data validation.	Apply updates per vendor instructions.	2022-07-18	
CVE-2021-30533	Google	Chromium	Google Chromium Security Bypass Vulnerability	2022-06-27	Insufficient policy enforcement in the PopupBlocker for Chromium allows an attacker to remotely bypass security mechanisms. This vulnerability impacts web browsers using Chromium such as Chrome and Edge.	Apply updates per vendor instructions.	2022-07-18	
CVE-2021-4034	Red Hat	Polkit	Red Hat Polkit Out-of-Bounds Read and Write Vulnerability	2022-06-27	The Red Hat polkit pkexec utility contains an out-of-bounds read and write vulnerability which allows for privilege escalation with administrative rights.	Apply updates per vendor instructions.	2022-07-18	
CVE-2021-30983	Apple	iOS and iPadOS	Apple iOS and iPadOS Buffer Overflow Vulnerability	2022-06-27	Apple iOS and iPadOS contain a buffer overflow vulnerability that could allow an application to execute code with kernel privileges.	Apply updates per vendor instructions.	2022-07-18	
CVE-2020-3837	Apple	Multiple Products	Apple Multiple Products Memory Corruption Vulnerability	2022-06-27	Apple iOS, iPadOS, macOS, tvOS, and watchOS contain a memory corruption vulnerability that could allow an application to execute code with kernel privileges.	Apply updates per vendor instructions.	2022-07-18	
CVE-2020-9907	Apple	Multiple Products	Apple Multiple Products Memory Corruption Vulnerability	2022-06-27	Apple iOS, iPadOS, and tvOS contain a memory corruption vulnerability that could allow an application to execute code with kernel privileges.	Apply updates per vendor instructions.	2022-07-18	
CVE-2019-8605	Apple	Multiple Products	Apple Multiple Products Use-After-Free Vulnerability	2022-06-27	A use-after-free vulnerability in Apple iOS, macOS, tvOS, and watchOS could allow a malicious application to execute code with system privileges.	Apply updates per vendor instructions.	2022-07-18	
CVE-2018-4344	Apple	Multiple Products	Apple Multiple Products Memory Corruption Vulnerability	2022-06-27	Apple iOS, macOS, tvOS, and watchOS contain a memory corruption vulnerability which can allow for code execution.	Apply updates per vendor instructions.	2022-07-18	