



CVE-2022-23008

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-23008
State	PUBLIC
Assigner	f5sirt@f5.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-25 20:15:00 UTC
Updated	2023-06-27 19:02:00 UTC
Description	On NGINX Controller API Management versions 3.18.0-3.19.0, an authenticated attacker with access to the "user" or "admin" role can exploit a vulnerability in the API to perform a Denial of Service (DoS) attack. The vulnerability is caused by a buffer overflow in the API when processing a request with a large payload. The attacker can send a request with a payload size that exceeds the buffer limit, causing the API to crash and the service to become unavailable. This vulnerability affects all versions of NGINX Controller API Management from 3.18.0 to 3.19.0. F5 has released a patch for this vulnerability in version 3.19.1. Users are advised to upgrade to the patched version as soon as possible.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Nginx Controller Api Management	All	All	All	All

References

Reference	Source	Link	Tags
support.f5.com/csp/article/K57735782	MISC	support.f5.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report