



CVE-2018-6667

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2018-6667
State	PUBLIC
Assigner	psirt@mcafee.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-26 17:29:00 UTC
Updated	2023-11-07 03:00:00 UTC
Description	Authentication Bypass vulnerability in the administrative user interface in McAfee Web Gateway 7.8.1.0 through 7.8.1.5 allo

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mcafee	Mcafee Web Gateway	All	All	All	All

References

Reference

- McAfee Web Gateway JMX Service Lets Remote Users Execute Arbitrary Code on the Target System - SecurityTracker
- McAfee Security Bulletin - Web Gateway update fixes several vulnerabilities (CVE-2018-6667, CVE-2018-1124, CVE-2017-12940, CVE-2017-
- McAfee Web Gateway CVE-2018-6667 Authentication Bypass Vulnerability
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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