



CVE-2018-5544

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

Summary

CVE	CVE-2018-5544
State	PUBLIC
Assigner	f5sirt@f5.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-31 14:29:00 UTC
Updated	2018-10-10 19:26:00 UTC
Description	When the F5 BIG-IP APM 13.0.0-13.1.1 or 12.1.0-12.1.3 renders certain pages (pages with a logon agent or a confirm box)

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All

References

Reference	
support.f5.com/csp/article/K23024812	C
F5 BIG-IP APM Page Rendering Bug Lets Remote Users Obtain Potentially Sensitive Information on the Target System - SecurityTracker	S
F5 BIG-IP APM CVE-2018-5544 Information Disclosure Vulnerability	B
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

378014 F5 BIG-IP Access Policy Manager (APM) Information Disclosure Vulnerability cve-2018-5544 (K23024812)

© [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](#)