



CVE-2019-16414

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

Summary

CVE	CVE-2019-16414
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-30 13:15:00 UTC
Updated	2019-10-04 14:43:00 UTC
Description	A DOM based XSS in GFI Kerio Control v9.3.0 allows embedding of malicious code and manipulating the login page to sen

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gfi	Kerio Control	9.3.0	All	All	All
Application	Gfi	Kerio Control	9.3.0	All	All	All

References

Reference

- Full Disclosure: DOM based XSS (Login page) in "GFI Kerio Control" Firewalls v9.3.0 / CVE-2019-16414 - working exploit attached
- GFI Kerio Control 9.3.0 Cross Site Scripting ≈ Packet Storm
- YouTube
- Haxel0rd on Twitter: "Dropping #0day for GFI "Kerio Control" Firewalls v9.3.0. Escalating simple DOM based XSS to an advanced attack on cl
- 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.

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)