



CVE-2016-10152

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

Summary

CVE	CVE-2016-10152
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-28 14:59:00 UTC
Updated	2018-10-21 10:29:00 UTC
Description	The read_config_file function in lib/hesiod.c in Hesiod 3.2.1 falls back to the ".athena.mit.edu" default domain when opening

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hesiod Project	Hesiod	All	All	All	All

References

Reference	Source
hesiod: Root privilege escalation (GLSA 201805-01) — Gentoo Security	GEN
1332493 – (CVE-2016-10152) CVE-2016-10152 hesiod: Use of hard-coded unsafe configuration if configuration file cannot be opened	COM
oss-security - Re: CVE Request: two flaws in hesiod permitting privilege elevation	MLIS
Hesiod Security Bypass and Privilege Escalation Vulnerabilities	BID
Remove hard-coded default for RHS by nalind · Pull Request #10 · achernya/hesiod · GitHub	COM
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[671394](#) EulerOS Security Update for hesiod (EulerOS-SA-2022-1325)

[671434](#) EulerOS Security Update for hesiod (EulerOS-SA-2022-1348)

© [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](#)