# 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 | Sou |
|---|---|
| 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 | CON |
| 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 | CON |
| 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)

671697 EulerOS Security Update for hesiod (EulerOS-SA-2022-1729)



**Free CVE JSON API** cve.report/api

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