



CVE-2015-1492

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

Summary

CVE	CVE-2015-1492
State	PUBLIC
Assigner	secure@symantec.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-01 01:59:00 UTC
Updated	2017-09-21 01:29:00 UTC
Description	Untrusted search path vulnerability in the client in Symantec Endpoint Protection 12.1 before 12.1-RU6-MP1 allows local users to execute arbitrary code via a crafted file path.

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Symantec	Endpoint Protection Manager	12.1.0	All	All	All
Application	Symantec	Endpoint Protection Manager	12.1.0	All	All	All

References

Reference
Security Advisories Relating to Symantec Products - Symantec Endpoint Protection Multiple Issues - 2015-07-30T06:00:00 PDT Symantec
Symantec Endpoint Protection Clients CVE-2015-1492 Binary Planting Vulnerability
Symantec Endpoint Protection Multiple Flaws Let Remote Users Bypass Authenticated and Remote Authenticated Users Read/Write Files, Inj
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.

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