



CVE-2020-7940

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

Summary

CVE	CVE-2020-7940
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-23 21:15:00 UTC
Updated	2020-01-24 22:52:00 UTC
Description	Missing password strength checks on some forms in Plone 4.3 through 5.2.0 allow users to set weak passwords, leading to



Risk And Classification

Problem Types: CWE-521

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Plone	Plone	All	All	All	All

References

Reference
oss-security - Re: Plone security hotfix 20200121
20200121 — Plone: Enterprise Level CMS - Free and OpenSource - Community Driven - Secure
oss-security - Plone security hotfix 20200121
Password strength checks were not always checked. — Plone: Enterprise Level CMS - Free and OpenSource - Community Driven - Secure
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](#).

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