



CVE-2020-26214

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2020-26214
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-06 18:15:00 UTC
Updated	2020-11-17 21:08:00 UTC
Description	In Alerta before version 8.1.0, users may be able to bypass LDAP authentication if they provide an empty password when A

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
alerta-server · PyPI	MISC	pypi.org
RFC 4513 - Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms	MISC	tools.ietf.org
Merge pull request #1345 from alerta/fix-ldap-empty-bind · alerta/alerta@2bfa317 · GitHub	MISC	github.com
Disallow LDAP anonymous bind · Issue #1277 · alerta/alerta · GitHub	MISC	github.com
LDAP authentication bypass with empty password · Advisory · alerta/alerta · GitHub	CONFIRM	github.com
Do not allow LDAP login with empty password by satterly · Pull Request #1345 · alerta/alerta · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [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](#)