[gentoo-announce] [GLSA 202208-19] aiohttp: Open redi...

Article URL
www.securityhome.eu/mailings/mailing.php?mid=21232

Author
SecurityHome.eu

Published: 11 August 2022

- -
Gentoo Linux Security Advisory GLSA 202208-19
- -
https://security.gentoo.org/
- -

Severity: Low
Title: aiohttp: Open redirect vulnerability
Date: August 10, 2022
Bugs: #772932
ID: 202208-19

- -

Synopsis
========
An open redirect vulnerability has been discovered in aiohttp.

Background
==========
aiohttp is an asynchronous HTTP client/server framework for asyncio and
Python.

Affected packages
=================

	Package	Vulnerable	Unaffected
1	dev-python/aiohttp	< 3.7.4	>= 3.7.4

Description
===========
A bug in aiohttp.web_middlewares.normalize_path_middleware creates an

open redirect vulnerability.

Impact
======
An attacker use this vulnerability to craft a link that, while appearing to be a link to an aiohttp-based website, redirects users to an arbitrary attacker-controlled URL.

Workaround
==========
There is no known workaround at this time.

Resolution
==========
All aiohttp users should upgrade to the latest version:

```
  # emerge --sync
  # emerge --ask --oneshot --verbose ">=dev-python/aiohttp-3.7.4"
```

References
==========
[1] CVE-2021-21330
    https://nvd.nist.gov/vuln/detail/CVE-2021-21330
[2] GHSA-v6wp-4m6f-gcjg

Availability
============
This GLSA and any updates to it are available for viewing at
the Gentoo Security Website:

 https://security.gentoo.org/glsa/202208-19

Concerns?
=========
Security is a primary focus of Gentoo Linux and ensuring the
confidentiality and security of our users' machines is of utmost
importance to us. Any security concerns should be addressed to
security@gentoo.org or alternatively, you may file a bug at
https://bugs.gentoo.org.

License
=======

--===============1785603591585045768==Content-Type: application/pgp-signature; name="signature.asc"
Content-Description: OpenPGP digital signature
Content-Disposition: attachment; filename="signature.asc"