

## [gentoo-announce] [ GLSA 202208-18 ] Motion: Denial of ...

Article URL

[www.securityhome.eu/mailings/mailling.php?mid=21231](http://www.securityhome.eu/mailings/mailling.php?mid=21231)

Author

SecurityHome.eu

Published: 11 August 2022

---

-----  
Gentoo Linux Security Advisory

GLSA 202208-18

-----  
<https://security.gentoo.org/>  
-----

Severity: Low

Title: Motion: Denial of service

Date: August 10, 2022

Bugs: #760714

ID: 202208-18

-----

### Synopsis

=====

A vulnerability in Motion allows a remote attacker to cause denial of service.

### Background

=====

Motion is a program that monitors the video signal from one or more cameras and is able to detect motions.

### Affected packages

=====

Package	/	Vulnerable	/	Unaffected
1 media-video/motion		< 4.3.2		>= 4.3.2

### Description

=====

The Motion HTTP server does not correctly perform URL decoding. If the HTTP server receives a request for a URL containing an incomplete percent-encoded character, a flaw in parsing results in an infinite loop trying to parse the rest of the character, which eventually results in a denial of service condition when reading out-of-bounds.

#### Impact

=====

A remote attacker can trigger a denial of service condition in Motion.

#### Workaround

=====

There is no known workaround at this time.

#### Resolution

=====

All Motion users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=media-video/motion-4.3.2"
```

#### References

=====

[ 1 ] CVE-2020-26566  
<https://nvd.nist.gov/vuln/detail/CVE-2020-26566>

#### Availability

=====

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

<https://security.gentoo.org/glsa/202208-18>

#### 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](mailto:security@gentoo.org) or alternatively, you may file a bug at <https://bugs.gentoo.org>.

#### License

=====

Copyright 2022 Gentoo Foundation, Inc; referenced text belongs to its owner(s).

The contents of this document are licensed under the Creative Commons - Attribution / Share Alike license.

<https://creativecommons.org/licenses/by-sa/2.5>

--=====0919796106703903466==Content-Type:

application/pgp-signature;

name="signature.asc"

Content-Description: OpenPGP digital signature

Content-Disposition: attachment; filename="signature.asc"