



# Bug 2315719 (CVE-2024-9355) - CVE-2024-9355 golang-fips: Golang FIPS zeroed buffer [NEEDINFO]

**Keywords:** Security

**Reported:** 2024-09-30 17:59 UTC by OSIDB Bzimport

**Status:** NEW

**Modified:** 2026-01-03 08:28 UTC ([History](#))

**Alias:** CVE-2024-9355

**CC List:** 89 users ([show](#))

**Product:** Security Response

**Fixed In Version:**

**Component:** vulnerability

**Clone Of:**

**Environment:**

**Version:** unspecified

**Last Closed:**

**Embargoed:**

**Hardware:** All

**Flags:** debarshir: needinfo? (bzimport)  
debarshir: needinfo? (pdelbell)

**OS:** Linux

**Priority:** medium

**Severity:** medium

**Target Milestone:** ---

**Assignee:** Product Security DevOps Team

**QA Contact:**

**Docs Contact:**

**URL:**

**Whiteboard:**

**Depends On:**

**Blocks:**

**TreeView+** [depends on](#) / [blocked](#)

## Attachments [\(Terms of Use\)](#)

### Links

| System                 | ID                             | Private | Priority | Status | Summary | Last Updated            |
|------------------------|--------------------------------|---------|----------|--------|---------|-------------------------|
| Red Hat Product Errata | <a href="#">RHBA-2024:7521</a> | 0       | None     | None   | None    | 2024-10-02 14:47:36 UTC |
| Red Hat Product Errata | <a href="#">RHBA-2024:7565</a> | 0       | None     | None   | None    | 2024-10-03 12:43:23 UTC |
| Red Hat Product Errata | <a href="#">RHBA-2024:7571</a> | 0       | None     | None   | None    | 2024-10-03 01:28:47 UTC |

|                        |                                 |   |      |      |      |                         |
|------------------------|---------------------------------|---|------|------|------|-------------------------|
| Red Hat Product Errata | <a href="#">RHBA-2024:8335</a>  | 0 | None | None | None | 2024-10-22 17:36:50 UTC |
| Red Hat Product Errata | <a href="#">RHBA-2024:8701</a>  | 0 | None | None | None | 2024-10-31 08:14:25 UTC |
| Red Hat Product Errata | <a href="#">RHBA-2024:8966</a>  | 0 | None | None | None | 2024-11-06 14:47:47 UTC |
| Red Hat Product Errata | <a href="#">RHSA-2024:10133</a> | 0 | None | None | None | 2024-11-21 01:08:23 UTC |
| Red Hat Product Errata | <a href="#">RHSA-2024:7502</a>  | 0 | None | None | None | 2024-10-02 11:42:08 UTC |
| Red Hat Product Errata | <a href="#">RHSA-2024:7550</a>  | 0 | None | None | None | 2024-10-02 18:20:12 UTC |
| Red Hat Product Errata | <a href="#">RHSA-2024:8327</a>  | 0 | None | None | None | 2024-10-22 15:09:02 UTC |
| Red Hat Product Errata | <a href="#">RHSA-2024:8678</a>  | 0 | None | None | None | 2024-10-30 19:36:33 UTC |
| Red Hat Product Errata | <a href="#">RHSA-2024:8847</a>  | 0 | None | None | None | 2024-11-05 03:53:36 UTC |
| Red Hat Product Errata | <a href="#">RHSA-2024:9551</a>  | 0 | None | None | None | 2024-11-13 14:50:11 UTC |
| Red Hat Product Errata | <a href="#">RHSA-2025:2416</a>  | 0 | None | None | None | 2025-03-05 20:59:17 UTC |
| Red Hat Product Errata | <a href="#">RHSA-2025:7118</a>  | 0 | None | None | None | 2025-05-13 10:03:16 UTC |
| Red Hat Product Errata | <a href="#">RHSA-2025:7256</a>  | 0 | None | None | None | 2025-05-13 10:29:44 UTC |
| Red Hat                | <a href="#">RHSA-2025:7624</a>  | 0 | None | None | None | 2025-05-14              |

|                   |  |  |  |  |                 |
|-------------------|--|--|--|--|-----------------|
| Product<br>Errata |  |  |  |  | 17:48:55<br>UTC |
|-------------------|--|--|--|--|-----------------|

OSIDB Bzimport  2024-09-30 17:59:28 UTC[Description](#)

Binaries built with golang-1.21.13-3.el9\_4 and golang-1.21.13-2.module+el8.10.0+22329+6cd5c9c6 may intermittently return a zeroed buffer from (\*boringHMAC).Sum() in FIPS mode due to an uninitialized buffer length variable in the CGO bindings. This bug occurs randomly based on the stack layout at the time of the function call. It is not vulnerable to eg. buffer overflow attack because the underlying openssl routine checks the bounds of the buffer before writing to it. However, it may be possible to force a false positive match between non-equal hashes when comparing a trusted computed hmac sum to an untrusted input sum if an attacker is able to send a zeroed buffer in place of a pre-computed sum. It is also possible to force a derived key to be all zeros instead of an unpredictable value. This may have follow-on implications for the Go TLS stack.

Debarshi Ray 2024-10-01 23:50:34 UTC

[Comment 1](#)

(In reply to OSIDB Bzimport from [comment #0](#))  
> Binaries built with golang-1.21.13-3.el9\_4 and  
> golang-1.21.13-2.module+el8.10.0+22329+6cd5c9c6 may  
> intermittently return a zeroed buffer from  
(\*boringHMAC).Sum() in FIPS mode  
> due to an uninitialized buffer length variable in the CGO  
bindings.

What do these NEVRA numbers really mean? Does a Go binary have to be compiled with one of these exact NEVRAS to have this bug? Or older? Or newer?

errata-xmlrpc 2024-10-02 11:42:04 UTC

[Comment 3](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2024:7502 <https://access.redhat.com/errata/RHSA-2024:7502>

errata-xmlrpc 2024-10-02 18:20:07 UTC

[Comment 4](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2024:7550 <https://access.redhat.com/errata/RHSA-2024:7550>

Debarshi Ray 2024-10-09 23:28:26 UTC

[Comment 5](#)

I am still looking for someone who can answer [comment 1](#)

errata-xmlrpc 2024-10-22 15:08:57 UTC

[Comment 6](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2024:8327 <https://access.redhat.com/errata/RHSA-2024:8327>

errata-xmlrpc 2024-10-30 19:36:28 UTC

[Comment 7](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2024:8678 <https://access.redhat.com/errata/RHSA-2024:8678>

errata-xmlrpc 2024-11-05 03:53:32 UTC

[Comment 8](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2024:8847 <https://access.redhat.com/errata/RHSA-2024:8847>

errata-xmlrpc 2024-11-13 14:50:06 UTC

[Comment 9](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.4 Extended Update Support

Via RHSA-2024:9551 <https://access.redhat.com/errata/RHSA-2024:9551>

[2024:9551](#)

errata-xmlrpc 2024-11-21 01:08:18 UTC

[Comment 10](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7 Extended Lifecycle Support

Via RHSA-2024:10133 <https://access.redhat.com/errata/RHSA-2024:10133>

errata-xmlrpc 2025-03-05 20:59:12 UTC

[Comment 11](#)

This issue has been addressed in the following products:

Streams for Apache Kafka 2.9.0

Via RHSA-2025:2416 <https://access.redhat.com/errata/RHSA-2025:2416>

errata-xmlrpc 2025-05-13 10:03:09 UTC

[Comment 17](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2025:7118 <https://access.redhat.com/errata/RHSA-2025:7118>

errata-xmlrpc 2025-05-13 10:29:37 UTC

[Comment 18](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2025:7256 <https://access.redhat.com/errata/RHSA-2025:7256>

errata-xmlrpc 2025-05-14 17:48:49 UTC

[Comment 19](#)

This issue has been addressed in the following products:

Satellite Client 6 for RHEL 8  
Satellite Client 6 for RHEL 9  
Satellite Client 6 for RHEL 10

Via RHSA-2025:7624 <https://access.redhat.com/errata/RHSA-2025:7624>

---

Note

You need to [log in](#) before you can comment on or make changes to this bug.

