Bug 2330539 (CVE-2024-12085) - CVE-2024-12085 rsync: Info Leak via Uninitialized Stack Contents

Keywords: Security

Status: NEW

Alias: CVE-2024-12085

Deadline: 2025-01-14

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2337965 2337966 ~~2337967~~ ~~2337968~~ ~~2337969~~ ~~2337970~~

Blocks:

TreeView+ depends on / blocked

Reported: 2024-12-05 12:29 UTC by OSIDB Bzimport

Modified: 2025-07-16 05:35 UTC (History)

CC List: 5 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHBA-2025:0376	0	None	None	None	2025-01-16 14:02:58 UTC
Red Hat Product Errata	RHBA-2025:0387	0	None	None	None	2025-01-16 18:29:55 UTC
Red Hat	RHBA-2025:0388	0	None	None	None	2025-01-16

Product Errata						18:37:28 UTC
Red Hat Product Errata	RHBA-2025:0389	0	None	None	None	2025-01-16 18:43:00 UTC
Red Hat Product Errata	RHBA-2025:0496	0	None	None	None	2025-01-21 11:23:12 UTC
Red Hat Product Errata	RHBA-2025:0605	0	None	None	None	2025-01-22 12:21:00 UTC
Red Hat Product Errata	RHBA-2025:0611	0	None	None	None	2025-01-22 13:22:14 UTC
Red Hat Product Errata	RHBA-2025:0613	0	None	None	None	2025-01-22 13:58:52 UTC
Red Hat Product Errata	RHBA-2025:0670	0	None	None	None	2025-01-23 17:30:42 UTC
Red Hat Product Errata	RHBA-2025:0671	0	None	None	None	2025-01-23 17:31:20 UTC
Red Hat Product Errata	RHBA-2025:0696	0	None	None	None	2025-01-27 02:09:36 UTC
Red Hat Product Errata	RHBA-2025:0703	0	None	None	None	2025-01-27 11:39:02 UTC
Red Hat Product Errata	RHBA-2025:0704	0	None	None	None	2025-01-27 11:38:54 UTC
Red Hat Product Errata	RHBA-2025:0705	0	None	None	None	2025-01-27 11:41:46 UTC
Red Hat Product Errata	RHBA-2025:0706	0	None	None	None	2025-01-27 11:41:04 UTC
Red Hat Product Errata	RHBA-2025:0707	0	None	None	None	2025-01-27 11:40:26 UTC

Red Hat Product Errata	RHBA-2025:0708	0	None	None	None	2025-01-27 13:58:25 UTC
Red Hat Product Errata	RHBA-2025:0769	0	None	None	None	2025-01-28 14:25:17 UTC
Red Hat Product Errata	RHBA-2025:0788	0	None	None	None	2025-01-29 08:41:14 UTC
Red Hat Product Errata	RHBA-2025:0789	0	None	None	None	2025-01-29 09:19:45 UTC
Red Hat Product Errata	RHBA-2025:0891	0	None	None	None	2025-02-03 11:10:14 UTC
Red Hat Product Errata	RHBA-2025:0898	0	None	None	None	2025-02-03 15:16:12 UTC
Red Hat Product Errata	RHBA-2025:0899	0	None	None	None	2025-02-03 15:16:32 UTC
Red Hat Product Errata	RHBA-2025:1105	0	None	None	None	2025-02-06 04:26:20 UTC
Red Hat Product Errata	RHBA-2025:1106	0	None	None	None	2025-02-06 04:52:11 UTC
Red Hat Product Errata	RHBA-2025:1237	0	None	None	None	2025-02-10 16:09:30 UTC
Red Hat Product Errata	RHBA-2025:1248	0	None	None	None	2025-02-10 18:08:32 UTC
Red Hat Product Errata	RHBA-2025:1349	0	None	None	None	2025-02-12 14:53:22 UTC
Red Hat Product Errata	RHBA-2025:1398	0	None	None	None	2025-02-13 05:16:02 UTC
Red Hat	RHSA-2025:0324	0	None	None	None	2025-01-15

Product Errata						06:44:04 UTC
Red Hat Product Errata	RHSA-2025:0325	0	None	None	None	2025-01-15 06:36:21 UTC
Red Hat Product Errata	RHSA-2025:0637	0	None	None	None	2025-01-22 23:45:37 UTC
Red Hat Product Errata	RHSA-2025:0688	0	None	None	None	2025-01-27 01:25:55 UTC
Red Hat Product Errata	RHSA-2025:0714	0	None	None	None	2025-01-27 16:36:44 UTC
Red Hat Product Errata	RHSA-2025:0774	0	None	None	None	2025-01-28 18:46:15 UTC
Red Hat Product Errata	RHSA-2025:0787	0	None	None	None	2025-01-29 08:00:09 UTC
Red Hat Product Errata	RHSA-2025:0790	0	None	None	None	2025-01-29 10:51:14 UTC
Red Hat Product Errata	RHSA-2025:0849	0	None	None	None	2025-01-30 16:57:04 UTC
Red Hat Product Errata	RHSA-2025:0884	0	None	None	None	2025-02-03 01:03:29 UTC
Red Hat Product Errata	RHSA-2025:0885	0	None	None	None	2025-02-03 01:05:52 UTC
Red Hat Product Errata	RHSA-2025:1120	0	None	None	None	2025-02-11 11:31:29 UTC
Red Hat Product Errata	RHSA-2025:1123	0	None	None	None	2025-02-12 00:13:40 UTC
Red Hat Product Errata	RHSA-2025:1128	0	None	None	None	2025-02-12 03:43:28 UTC

Red Hat Product Errata	RHSA-2025:1227	0	None	None	None	2025-02-12 16:40:17 UTC
Red Hat Product Errata	RHSA-2025:1242	0	None	None	None	2025-02-13 02:11:24 UTC
Red Hat Product Errata	RHSA-2025:1451	0	None	None	None	2025-02-19 23:11:05 UTC
Red Hat Product Errata	RHSA-2025:2701	0	None	None	None	2025-03-20 07:01:29 UTC

OSIDB Bzimport 2024-12-05 12:29:53 UTC Description

```
The attacker can exploit this vulnerability to leak
uninitialized stack data byte by byte, potentially exposing
memory locations of critical data.It uses a buffer (sum2) on
the stack to store part of the checksum but does not
initialize this buffer. An attacker can manipulate the
checksum length (s2length) to cause a comparison between a
checksum and uninitialized memory. This allows an attacker to
leak one byte of uninitialized stack data at a time. Over
multiple requests, the attacker can leak up to MAX_DIGEST_LEN
- 8 bytes of sensitive data, which could help defeat Address
Space Layout Randomization (ASLR).
```

errata-xmlrpc 2025-01-15 06:36:20 UTC Comment 3

```
This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2025:0325 https://access.redhat.com/errata/RHSA-
2025:0325
```

errata-xmlrpc 2025-01-15 06:44:02 UTC Comment 4

```
This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2025:0324 https://access.redhat.com/errata/RHSA-
2025:0324
```

errata-xmlrpc 2025-01-22 23:45:36 UTC Comment 5

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.4 Extended Update Support

Via RHSA-2025:0637 https://access.redhat.com/errata/RHSA-2025:0637

errata-xmlrpc 2025-01-27 01:25:54 UTC Comment 6

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions

Via RHSA-2025:0688 https://access.redhat.com/errata/RHSA-2025:0688

errata-xmlrpc 2025-01-27 16:36:42 UTC Comment 7

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 7 Extended Lifecycle Support

Via RHSA-2025:0714 https://access.redhat.com/errata/RHSA-2025:0714

errata-xmlrpc 2025-01-28 18:46:14 UTC Comment 8

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.2 Extended Update Support

Via RHSA-2025:0774 https://access.redhat.com/errata/RHSA-2025:0774

errata-xmlrpc 2025-01-29 08:00:07 UTC Comment 9

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.8 Extended Update Support

Via RHSA-2025:0787 https://access.redhat.com/errata/RHSA-

2025:0787

errata-xmlrpc 2025-01-29 10:51:12 UTC Comment 10

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support
  Red Hat Enterprise Linux 8.6 Update Services for SAP Solutions
  Red Hat Enterprise Linux 8.6 Telecommunications Update Service

Via RHSA-2025:0790 https://access.redhat.com/errata/RHSA-2025:0790

errata-xmlrpc 2025-01-30 16:57:02 UTC Comment 11

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 6 Extended Lifecycle Support - EXTENSION

Via RHSA-2025:0849 https://access.redhat.com/errata/RHSA-2025:0849

errata-xmlrpc 2025-02-03 01:03:27 UTC Comment 12

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.2 Advanced Update Support

Via RHSA-2025:0884 https://access.redhat.com/errata/RHSA-2025:0884

errata-xmlrpc 2025-02-03 01:05:49 UTC Comment 13

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support
  Red Hat Enterprise Linux 8.4 Update Services for SAP Solutions
  Red Hat Enterprise Linux 8.4 Telecommunications Update Service

Via RHSA-2025:0885 https://access.redhat.com/errata/RHSA-2025:0885

errata-xmlrpc 2025-02-11 11:31:27 UTC Comment 15

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.17

Via RHSA-2025:1120 https://access.redhat.com/errata/RHSA-2025:1120

errata-xmlrpc 2025-02-12 00:13:39 UTC Comment 16

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.16

Via RHSA-2025:1123 https://access.redhat.com/errata/RHSA-2025:1123

errata-xmlrpc 2025-02-12 03:43:26 UTC Comment 17

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.15

Via RHSA-2025:1128 https://access.redhat.com/errata/RHSA-2025:1128

errata-xmlrpc 2025-02-12 16:40:15 UTC Comment 18

This issue has been addressed in the following products:

RHOL-5.9-RHEL-9

Via RHSA-2025:1227 https://access.redhat.com/errata/RHSA-2025:1227

errata-xmlrpc 2025-02-13 02:11:23 UTC Comment 19

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.12

Via RHSA-2025:1242 https://access.redhat.com/errata/RHSA-2025:1242

errata-xmlrpc 2025-02-19 23:11:03 UTC Comment 21

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.14

Via RHSA-2025:1451 https://access.redhat.com/errata/RHSA-2025:1451

errata-xmlrpc 2025-03-20 07:01:27 UTC Comment 23

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.13

Via RHSA-2025:2701 https://access.redhat.com/errata/RHSA-2025:2701

Note

You need to log in before you can comment on or make changes to this bug.