Bug 2262921 (CVE-2024-1394) - CVE-2024-1394 golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads

Keywords: Security ×

Status: NEW

Alias: CVE-2024-1394

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2262923 2262924 2262925 2262926 2262927 2262928 2262929 2262930 2262931 2262932 2262933 2262934 2262935 2262936 2262937 2262949 2262950 2262951 2262952 2262953 2262954 2262955 2262956 2279584

Blocks: 2262922

TreeView+ depends on / blocked

Reported: 2024-02-06 06:06 UTC by Avinash Hanwate

Modified: 2026-04-18 08:28 UTC (History)

CC List: 112 users (show)

Fixed In Version: github.com/golang-fips/openssl/v2 2.0.1, github.com/microsoft/go-crypto-openssl/openssl 0.2.9

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat	RHBA-2024:1478	0	None	None	None	2024-03-25

Product Errata						01:07:31 UTC
Red Hat Product Errata	RHBA-2024:1586	0	None	None	None	2024-04-01 19:37:06 UTC
Red Hat Product Errata	RHBA-2024:1656	0	None	None	None	2024-04-03 06:43:36 UTC
Red Hat Product Errata	RHBA-2024:1661	0	None	None	None	2024-04-03 10:23:34 UTC
Red Hat Product Errata	RHBA-2024:1929	0	None	None	None	2024-04-18 20:25:57 UTC
Red Hat Product Errata	RHBA-2024:4506	0	None	None	None	2024-07-11 13:25:18 UTC
Red Hat Product Errata	RHBA-2024:4688	0	None	None	None	2024-07-22 06:18:45 UTC
Red Hat Product Errata	RHBA-2024:4692	0	None	None	None	2024-07-22 07:00:49 UTC
Red Hat Product Errata	RHBA-2024:5335	0	None	None	None	2024-08-13 17:32:41 UTC
Red Hat Product Errata	RHSA-2024:0045	0	None	None	None	2024-06-27 13:01:00 UTC
Red Hat Product Errata	RHSA-2024:1472	0	None	None	None	2024-03-21 15:40:04 UTC
Red Hat Product Errata	RHSA-2024:1561	0	None	None	None	2024-04-02 21:54:23 UTC
Red Hat Product Errata	RHSA-2024:1563	0	None	None	None	2024-04-02 21:38:09 UTC
Red Hat Product Errata	RHSA-2024:1566	0	None	None	None	2024-04-03 16:19:27 UTC

Red Hat Product Errata	RHSA-2024:1567	0	None	None	None	2024-04-03 16:00:27 UTC
Red Hat Product Errata	RHSA-2024:1574	0	None	None	None	2024-04-03 07:36:38 UTC
Red Hat Product Errata	RHSA-2024:1640	0	None	None	None	2024-04-02 19:30:42 UTC
Red Hat Product Errata	RHSA-2024:1644	0	None	None	None	2024-04-02 20:50:11 UTC
Red Hat Product Errata	RHSA-2024:1646	0	None	None	None	2024-04-02 20:50:25 UTC
Red Hat Product Errata	RHSA-2024:1763	0	None	None	None	2024-04-18 18:22:40 UTC
Red Hat Product Errata	RHSA-2024:1897	0	None	None	None	2024-04-26 20:11:20 UTC
Red Hat Product Errata	RHSA-2024:2562	0	None	None	None	2024-04-30 14:39:38 UTC
Red Hat Product Errata	RHSA-2024:2568	0	None	None	None	2024-04-30 14:40:41 UTC
Red Hat Product Errata	RHSA-2024:2569	0	None	None	None	2024-04-30 14:41:34 UTC
Red Hat Product Errata	RHSA-2024:2729	0	None	None	None	2024-05-22 20:38:35 UTC
Red Hat Product Errata	RHSA-2024:2730	0	None	None	None	2024-05-22 20:41:55 UTC
Red Hat Product Errata	RHSA-2024:2767	0	None	None	None	2024-05-22 20:11:58 UTC
Red Hat	RHSA-2024:3265	0	None	None	None	2024-05-22

Product Errata						11:40:43 UTC
Red Hat Product Errata	RHSA-2024:4146	0	None	None	None	2024-06-27 00:20:21 UTC
Red Hat Product Errata	RHSA-2024:4371	0	None	None	None	2024-07-08 13:17:45 UTC
Red Hat Product Errata	RHSA-2024:4378	0	None	None	None	2024-07-08 14:31:08 UTC
Red Hat Product Errata	RHSA-2024:4379	0	None	None	None	2024-07-08 14:42:31 UTC
Red Hat Product Errata	RHSA-2024:4502	0	None	None	None	2024-07-15 13:27:32 UTC
Red Hat Product Errata	RHSA-2024:4581	0	None	None	None	2024-07-16 18:40:48 UTC
Red Hat Product Errata	RHSA-2024:4591	0	None	None	None	2024-07-17 13:13:18 UTC
Red Hat Product Errata	RHSA-2024:4672	0	None	None	None	2024-07-22 01:10:23 UTC
Red Hat Product Errata	RHSA-2024:4699	0	None	None	None	2024-07-25 14:16:24 UTC
Red Hat Product Errata	RHSA-2024:4761	0	None	None	None	2024-07-23 16:23:10 UTC
Red Hat Product Errata	RHSA-2024:4762	0	None	None	None	2024-07-23 16:23:19 UTC
Red Hat Product Errata	RHSA-2024:4960	0	None	None	None	2024-08-07 10:51:59 UTC
Red Hat Product Errata	RHSA-2024:5258	0	None	None	None	2024-08-13 00:37:47 UTC

Red Hat Product Errata	RHSA-2024:5634	0	None	None	None	2024-08-20 16:07:35 UTC
Red Hat Product Errata	RHSA-2024:7262	0	None	None	None	2024-09-26 18:33:14 UTC
Red Hat Product Errata	RHSA-2025:7118	0	None	None	None	2025-05-13 10:03:13 UTC

Avinash Hanwate 2024-02-06 06:06:25 UTC Description

```
A memory leak flaw was found in the RSA encrypting/decrypting
code which might lead to a resource exhaustion vulnerability,
as it is theoretically exploitable using attacker-controlled
inputs. The memory leak happens in github.com/golang-
fips/openssl/openssl/rsa.go#L113. The objects leaked are pkey
and ctx. That function uses named return parameters to free
pkey and ctx if there is an error initializing the context or
setting the different properties. Unfortunately, notice that
all the return statements related to error cases follow the
"return nil, nil, fail(...)" pattern, which means that pkey
and ctx will be nil inside the deferred function that should
free them.
```

Tom Sweeney 2024-02-13 19:18:29 UTC Comment 3

```
Any thoughts on a fixed in version yet?  It would be helpful,
for the moment, to know the module that's affected.
```

Anten Skrabec 2024-03-20 21:39:58 UTC Comment 12

```
populated fixed in field
```

Tom Sweeney 2024-03-21 00:53:46 UTC Comment 13

```
Thanks for the update.
```

errata-xmlrpc 2024-03-21 15:39:57 UTC Comment 16

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2024:1472 https://access.redhat.com/errata/RHSA-2024:1472

errata-xmlrpc 2024-04-02 19:30:35 UTC Comment 19

This issue has been addressed in the following products:

  Red Hat Ansible Automation Platform 2.4 for RHEL 9
  Red Hat Ansible Automation Platform 2.4 for RHEL 8

Via RHSA-2024:1640 https://access.redhat.com/errata/RHSA-2024:1640

errata-xmlrpc 2024-04-02 20:50:05 UTC Comment 20

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2024:1644 https://access.redhat.com/errata/RHSA-2024:1644

errata-xmlrpc 2024-04-02 20:50:20 UTC Comment 21

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2024:1646 https://access.redhat.com/errata/RHSA-2024:1646

errata-xmlrpc 2024-04-02 21:38:01 UTC Comment 22

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.15

Via RHSA-2024:1563 https://access.redhat.com/errata/RHSA-2024:1563

errata-xmlrpc 2024-04-02 21:54:18 UTC Comment 23

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.15

Via RHSA-2024:1561 https://access.redhat.com/errata/RHSA-2024:1561

errata-xmlrpc 2024-04-03 07:36:31 UTC Comment 24

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.12

Via RHSA-2024:1574 https://access.redhat.com/errata/RHSA-2024:1574

errata-xmlrpc 2024-04-03 16:00:19 UTC Comment 25

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.14

Via RHSA-2024:1567 https://access.redhat.com/errata/RHSA-2024:1567

errata-xmlrpc 2024-04-03 16:19:19 UTC Comment 26

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.14

Via RHSA-2024:1566 https://access.redhat.com/errata/RHSA-2024:1566

errata-xmlrpc 2024-04-18 18:22:33 UTC Comment 27

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.13

Via RHSA-2024:1763 https://access.redhat.com/errata/RHSA-

2024:1763

errata-xmlrpc 2024-04-26 20:11:14 UTC Comment 28

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.14

Via RHSA-2024:1897 https://access.redhat.com/errata/RHSA-2024:1897

errata-xmlrpc 2024-04-30 14:39:32 UTC Comment 29

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2024:2562 https://access.redhat.com/errata/RHSA-2024:2562

errata-xmlrpc 2024-04-30 14:40:35 UTC Comment 30

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2024:2568 https://access.redhat.com/errata/RHSA-2024:2568

errata-xmlrpc 2024-04-30 14:41:27 UTC Comment 31

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2024:2569 https://access.redhat.com/errata/RHSA-2024:2569

errata-xmlrpc 2024-05-22 11:40:34 UTC Comment 33

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2024:3265 https://access.redhat.com/errata/RHSA-2024:3265

errata-xmlrpc 2024-05-22 20:11:48 UTC Comment 34

This issue has been addressed in the following products:

Red Hat OpenStack Platform 17.1 for RHEL 8

Via RHSA-2024:2767 https://access.redhat.com/errata/RHSA-2024:2767

errata-xmlrpc 2024-05-22 20:38:26 UTC Comment 35

This issue has been addressed in the following products:

Red Hat OpenStack Platform 17.1 for RHEL 9

Via RHSA-2024:2729 https://access.redhat.com/errata/RHSA-2024:2729

errata-xmlrpc 2024-05-22 20:41:45 UTC Comment 36

This issue has been addressed in the following products:

Red Hat OpenStack Platform 17.1 for RHEL 9

Via RHSA-2024:2730 https://access.redhat.com/errata/RHSA-2024:2730

Anten Skrabec 2024-06-11 20:05:38 UTC Comment 39

filed rhel-9 z-stream trackers per https://issues.redhat.com/browse/RHEL-24310?focusedId=24906983&page=com.atlassian.jira.plugin.system.issuetabpanels:comment-tabpanel#comment-24906983

Anten Skrabec 2024-06-11 21:28:00 UTC Comment 40

wrong component, refiling for rhel-9 containernetworking-plugins

errata-xmlrpc 2024-06-27 00:20:12 UTC Comment 45

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.2 Extended Update Support

Via RHSA-2024:4146 https://access.redhat.com/errata/RHSA-2024:4146

errata-xmlrpc 2024-06-27 13:00:52 UTC Comment 46

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.16

Via RHSA-2024:0045 https://access.redhat.com/errata/RHSA-2024:0045

errata-xmlrpc 2024-07-08 13:17:36 UTC Comment 48

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2024:4371 https://access.redhat.com/errata/RHSA-2024:4371

errata-xmlrpc 2024-07-08 14:30:59 UTC Comment 49

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2024:4378 https://access.redhat.com/errata/RHSA-2024:4378

errata-xmlrpc 2024-07-08 14:42:24 UTC Comment 50

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2024:4379 https://access.redhat.com/errata/RHSA-2024:4379

errata-xmlrpc 2024-07-15 13:27:24 UTC Comment 52

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2024:4502 https://access.redhat.com/errata/RHSA-2024:4502

errata-xmlrpc 2024-07-16 18:40:41 UTC Comment 53

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions

Via RHSA-2024:4581 https://access.redhat.com/errata/RHSA-2024:4581

errata-xmlrpc 2024-07-17 13:13:09 UTC Comment 54

This issue has been addressed in the following products:

  RHODF-4.16-RHEL-9

Via RHSA-2024:4591 https://access.redhat.com/errata/RHSA-2024:4591

errata-xmlrpc 2024-07-22 01:10:14 UTC Comment 55

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions

Via RHSA-2024:4672 https://access.redhat.com/errata/RHSA-2024:4672

errata-xmlrpc 2024-07-23 16:23:02 UTC Comment 57

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2024:4761 https://access.redhat.com/errata/RHSA-2024:4761

errata-xmlrpc 2024-07-23 16:23:09 UTC Comment 58

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2024:4762 https://access.redhat.com/errata/RHSA-2024:4762

errata-xmlrpc 2024-07-25 14:16:15 UTC Comment 59

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.15

Via RHSA-2024:4699 https://access.redhat.com/errata/RHSA-2024:4699

errata-xmlrpc 2024-08-07 10:51:52 UTC Comment 60

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.14

Via RHSA-2024:4960 https://access.redhat.com/errata/RHSA-2024:4960

errata-xmlrpc 2024-08-13 00:37:38 UTC Comment 61

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2024:5258 https://access.redhat.com/errata/RHSA-

2024:5258

errata-xmlrpc 2024-08-20 16:07:27 UTC Comment 62

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.2 Extended Update Support

Via RHSA-2024:5634 https://access.redhat.com/errata/RHSA-2024:5634

errata-xmlrpc 2024-09-26 18:33:05 UTC Comment 63

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2024:7262 https://access.redhat.com/errata/RHSA-2024:7262

errata-xmlrpc 2025-05-13 10:03:03 UTC Comment 73

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

Note

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