Final - K37451543: TMM vulnerability CVE-2021-23007

Security Advisory

Original Publication Date: Mar 19, 2021
Updated Date: Jul 19, 2021

This article is marked as 'Final' because the security issue described in this article either affected F5 products at one time and was resolved or it never affected F5 products. Unless new information is discovered, F5 will no longer update the article.

Security Advisory Description

When the Traffic Management Microkernel (TMM) process handles certain undisclosed traffic, it may start dropping all fragmented IP traffic. (CVE-2021-23007)

Impact

TMM incorrectly determines that the fragment memory limit has been reached and drops all fragments it receives, disrupting traffic to the BIG-IP system.

You can determine if your system is impacted by running the **tmctl ip_stat** command from the BIG-IP command line and reviewing the output for an unusually large value in the **frag_bytes_used** column for a given TMM. You may observe that some TMM processes have high values and others do not. For example:

```
  rx_frag rx_frag_dropped err_frag_mem_limit_reached      frag_bytes_used
-------- --------------- -------------------------- --------------------
46406517             508                          0                    0

  rx_frag rx_frag_dropped err_frag_mem_limit_reached      frag_bytes_used
-------- --------------- -------------------------- --------------------
44739031             217                          0                    0

  rx_frag rx_frag_dropped err_frag_mem_limit_reached      frag_bytes_used
-------- --------------- -------------------------- --------------------
39322744         8404728                    8404628 18446744073709547072

  rx_frag rx_frag_dropped err_frag_mem_limit_reached      frag_bytes_used
-------- --------------- -------------------------- --------------------
33528060        15659496                   15659334 18446744073709547072

  rx_frag rx_frag_dropped err_frag_mem_limit_reached      frag_bytes_used
-------- --------------- -------------------------- --------------------
46712180             157                          0                    0

  rx_frag rx_frag_dropped err_frag_mem_limit_reached      frag_bytes_used
-------- --------------- -------------------------- --------------------
38912369        10588696                   10588558 18446744073709547072
```

Security Advisory Status

F5 Product Development has assigned ID 1002561 (BIG-IP) to this vulnerability.

To determine if your product and version have been evaluated for this vulnerability, refer to the **Applies to (see versions)** box. To determine if your release is known to be vulnerable, the components or features that are affected by the vulnerability, and for information about releases, point releases, or hotfixes that address the vulnerability, refer to the following table. For more information about security advisory versioning, refer to K51812227: Understanding security advisory versioning.

***Note**: After a fix is introduced for a vulnerable version, that fix applies to all subsequent point releases for that version and no additional fixes for that version will be listed in the table. For example, when a fix is introduced in 14.1.2.3, the fix applies to 14.1.2.4 and all later point releases.*

Product	Branch	Versions known to be vulnerable	Fixes introduced in	Severity	CVSSv3 score[1]	Vulnerable component or feature
BIG-IP (all modules)	16.x	16.0.1.1	16.1.0 Hotfix-BIGIP-16.0.1.1.9.6-ENG.iso[2]	Medium	5.3	TMM (IP Fragment Handling)
	15.x	None	Not applicable			
	14.x	14.1.4	14.1.4.1, Hotfix-BIGIP-14.1.4.0.120.11-ENG.iso[2]			
	13.x	None	Not applicable			
	12.x	None	Not applicable			
	11.x	None	Not applicable			
BIG-IQ Centralized Management	8.x	None	Not applicable	Not vulnerable	None	None
	7.x	None	Not applicable			
	6.x	None	Not applicable			
F5OS	1.x	None	Not applicable	Not vulnerable	None	None
Traffix SDC	5.x	None	Not applicable	Not vulnerable	None	None

[1]The CVSSv3 score link takes you to a resource outside of AskF5, and it is possible that the document may be removed without our knowledge.

[2]You can download engineering hotfix releases from the following locations:

- Engineering hotfix for 16.0.1.1: https://downloads.f5.com/esd/ecc.sv?sw=BIG-IP&pro=big-ip_v16.x&ver=16.0.1&container=HotFix-BIGIP-16.0.1.1.9.6-EHF9

- Engineering hotfix for 14.1.4: https://downloads.f5.com/esd/ecc.sv?sw=BIG-IP&pro=big-ip_v14.x&ver=14.1.4&container=HotFix-BIGIP-14.1.4.0.120.11-EHF120

Recommended Actions

If you are running a version listed in the **Versions known to be vulnerable** column, you can eliminate this vulnerability by installing a version listed in the **Fixes introduced in** column. If the **Fixes introduced in** column does not list a version for your branch, then no update candidate currently exists for that branch and F5 recommends upgrading to a version with the fix (refer to the table).

If the **Fixes introduced in** column lists a version prior to the one you are running, in the same branch, then your version should have the fix.

Mitigation

You can restart the TMM process to recover from the condition; however, this is not a permanent fix. To do so, perform the following procedure:

Impact of procedure: *Performing the following procedure causes a temporary traffic disruption while the TMM process restarts. You should perform this procedure only during a scheduled maintenance period.*

1. Log in to the TMOS Shell (**tmsh**) by entering the following command:
   ```
   tmsh
   ```
2. To restart the TMM process, enter the following command:
   ```
   restart /sys service tmm
   ```

Acknowledgements

This issue was discovered by F5.

Supplemental Information

- K21521909: Determine if your BIG-IP system is impacted by CVE-2021-23007
- K41942608: Overview of security advisory articles
- K4602: Overview of the F5 security vulnerability response policy
- K4918: Overview of the F5 critical issue hotfix policy
- K9502: BIG-IP hotfix and point release matrix
- K13123: Managing BIG-IP product hotfixes (11.x - 16.x)
- K167: Downloading software and firmware from F5
- K9970: Subscribing to email notifications regarding F5 products
- K9957: Creating a custom RSS feed to view new and updated documents

Applies to:

Product: BIG-IQ, BIG-IQ Centralized Management
8.0.0, 7.1.0, 7.0.0, 6.1.0, 6.0.1, 6.0.0

Product: BIG-IP, BIG-IP AFM, BIG-IP Analytics, BIG-IP APM, BIG-IP ASM, BIG-IP DNS, BIG-IP FPS, BIG-IP GTM, BIG-IP Link Controller, BIG-IP LTM, BIG-IP PEM, BIG-IP AAM
16.1.0, 16.0.1, 16.0.0, 15.1.2, 15.1.1, 15.1.0, 14.1.4, 14.1.3, 14.1.2, 14.1.0, 13.1.3, 13.1.1, 13.1.0, 12.1.5, 12.1.4, 12.1.3, 12.1.2, 12.1.1, 12.1.0, 11.6.5, 11.6.4, 11.6.3, 11.6.2, 11.6.1

Product: F5OS
1.1.2, 1.1.1, 1.1.0

Product: Traffix SDC
5.1.0

Product: F5 App Protect, F5 SSL Orchestrator, F5 DDoS Hybrid Defender
16.0.1, 16.0.0, 15.1.1, 15.1.0, 14.1.4, 14.1.2, 14.1.0, 13.1.0