AskF5 Home / K66510514

K66510514: TMM vulnerability CVE-2022-34862

Security Advisory

Original Publication Date: Aug 03, 2022

Security Advisory Description

`When an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate.` (CVE-2022-34862)

Impact

This vulnerability affects systems with one or more of the following configurations.

Affected configurations

BIG-IP APM

This vulnerability affects a virtual server associated with a BIG-IP APM profile. All BIG-IP APM use cases are vulnerable.

BIG-IP ASM

This vulnerability affects only BIG-IP ASM Risk Engine use cases. BIG-IP ASM Risk Engine is currently available only to Early Access (EA) customers and requires a special license.

BIG-IP PEM

This vulnerability affects BIG-IP PEM systems that use:

- URL filtering with the Websense database license activated.
- One or more virtual servers that perform URL categorization and use one of the following:
    - An iRule
    - A local traffic policy
    - A BIG-IP PEM policy

Secure Web Gateway

This vulnerability affects all F5 Secure Web Gateway (SWG) use cases. URL categorization is fundamental to the operation of SWG. SWG requires a separate subscription.

SSL Orchestrator

This vulnerability affects all systems that use the SSL Orchestrator Categorization macro.

BIG-IP (all modules)

This vulnerability affects all BIG-IP system modules that use one or more of the following configurations:

- URL filtering with the Websense database license activated.
- A virtual server associated with an HTTP profile and a local traffic policy with a rule condition that has the following options enabled: **HTTP URI** or **HTTP Referer** and **Use normalized URI**.
  ***Note**: The **Use normalized URI** option is disabled by default.*

  For more information about HTTP profiles and local traffic policy rules, refer to K40243113: Overview of the HTTP profile and K04597703: Overview of the Local Traffic Policies feature (12.1.0 and later) respectively.

  For example, in the following configuration, the local traffic policy is vulnerable:

  ```
  ltm policy /Common/K56715231 {
      requires { http http-connect }
      rules {
          VULN_RULE01 {
              conditions {
                  0 {
                      http-uri
                      proxy-connect
                      normalized
                      values { VULN_URI_STRING }
                  }
              }
          }
          VULN_RULE02 {
              conditions {
                  0 {
                      http-referer
                      proxy-connect
                      normalized
                      values { VULN_REF_STRING }
                  }
              }
              ordinal 1
          }
      }
      strategy /Common/first-match
  }
  ```

- A virtual server associated with an HTTP profile and an iRule that uses any of the following commands with the **-normalized** switch:

  - **HTTP::uri**
  - **HTTP::query**
  - **HTTP::path**

For example, the following iRule is vulnerable:

```
when HTTP_REQUEST {
      if { ([HTTP::uri -normalized] starts_with "/vulnerable")} {
           log local0.error "K56715231 URI example"
      } elseif { ([HTTP::query -normalized] starts_with "/vulnerable")} {
           log local0.error "K56715231  Query example"
      } elseif { ([HTTP::path -normalized] starts_with "/vulnerable")} {
           log local0.error "K56715231  Path example"
      }
 }
```

Identify whether your system has URL filtering with the Websense database license activated

You can identify whether your BIG-IP system has URL filtering with the Websense database license activated by checking the **/var/log/tmm** log file during restart. When you have this feature, you see a log entry similar to the following example:

```
tmm:<13> Apr  18 06:14:15 bigip.local notice URLCAT_LIB:
urlcat_websense_license_callback/984: WEBSENSE DB is licensed
```

This log entry displays only when you set the **tmm.lib.urlcat.log.level** BIG-IP system database variable to **Debug**.

Note*: If you think your system is compromised, refer to K11438344: Considerations and guidance when you suspect a security compromise on a BIG-IP system.*

Security Advisory Status

F5 Product Development has assigned IDs 1073357 and 1073841 (BIG-IP) to this vulnerability. This issue has been classified as CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop').

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 given minor branch, that fix applies to all subsequent maintenance and point releases for that branch, and no additional fixes for that branch will be listed in the table. For example, when a fix is introduced in 14.1.2.3, the fix also applies to 14.1.2.4, and all later 14.1.x releases (14.1.3.x., 14.1.4.x). For more information, refer to K51812227: Understanding security advisory versioning. Additionally, software versions preceding those listed in the* ***Applies to (see versions)*** *box of this article have reached the End of Technical Support (EoTS) phase of their lifecycle and are no longer evaluated for security issues. For more information, refer to the* ***Security hotfixes*** *section of K4602: Overview of the F5 security vulnerability response policy.*

Product	Branch	Versions known to be vulnerable[1]	Fixes introduced in	Severity	CVSSv3 score[2]	Vulnerable component or feature
BIG-IP (all modules)	17.x	None	17.0.0	High	7.5	TMM
	16.x	16.1.0 - 16.1.3	16.1.3.1			

	15.x	15.1.0 - 15.1.6	15.1.6.1			
	14.x	14.1.0 - 14.1.4	14.1.5			
	13.x	13.1.0 - 13.1.5	None			
BIG-IP SPK	1.x	None	Not applicable	Not vulnerable	None	None
BIG-IQ Centralized Management	8.x	None	Not applicable	Not vulnerable	None	None
	7.x	None	Not applicable			
F5OS-A	1.x	None	Not applicable	Not vulnerable	None	None
F5OS-C	1.x	None	Not applicable	Not vulnerable	None	None
Traffix SDC	5.x	None	Not applicable	Not vulnerable	None	None

[1] *F5 evaluates only software versions that have not yet reached the End of Technical Support (EoTS) phase of their lifecycle.*

[2] *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.*

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

F5 recommends you configure the BIG-IP systems with high availability (HA) to lessen the impact of the vulnerability.

- Configure systems with HA clustering. For more information, refer to K02234544: Manually setting up device service clustering.
- Configure the HA table to take specific actions. For more information, refer to K9231: Overview of BIG-IP daemon heartbeat failsafe.

Acknowledgements

This issue was discovered internally by F5.

Supplemental Information

- K41942608: Overview of security advisory articles
- K4602: Overview of the F5 security vulnerability response policy
- K4918: Overview of the F5 critical issue hotfix policy
- K8986: F5 product support policies
- K9502: BIG-IP hotfix and point release matrix
- K13123: Managing BIG-IP product hotfixes (11.x - 17.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
8.2.0, 8.1.0, 8.0.0, 7.1.0, 7.0.0

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
17.0.0, 16.1.3, 16.1.2, 16.1.1, 16.1.0, 15.1.6, 15.1.5, 15.1.4, 15.1.3, 15.1.2, 15.1.1, 15.1.0, 14.1.5, 14.1.4, 14.1.3, 14.1.2, 14.1.0, 13.1.5, 13.1.4, 13.1.3, 13.1.1, 13.1.0

Product: F5OS, F5OS-A, F5OS-C
1.3.2, 1.3.1, 1.3.0, 1.2.2, 1.2.1, 1.2.0, 1.1.4, 1.1.3, 1.1.2, 1.1.1, 1.1.0, 1.0.1, 1.0.0

Product: 5G Products, BIG-IP SPK
1.5.0

Product: Traffix SDC
5.2.0, 5.1.0

Product: F5 App Protect, F5 SSL Orchestrator, F5 DDoS Hybrid Defender
17.0.0, 16.1.3, 16.1.1, 16.1.0, 15.1.1, 15.1.0, 14.1.4, 14.1.2, 14.1.0