Severity

High

Analysis Summary

CVE-2022-25946 CVSS:8.7

F5 BIG-IP (Advanced WAF, APM, ASM) and Guided Configuration (GC) could allow a remote authenticated attacker to bypass security restrictions, caused by the missing of integrity check. By sending a specially-crafted request, an attacker could exploit this vulnerability to bypass Appliance mode restrictions.

CVE-2022-25990 CVSS:5.3

F5 F5OS-A could allow a remote attacker to obtain sensitive information, caused by an unspecified flaw. By sending a specially-crafted request, an attacker could exploit this vulnerability to obtain the Docker registry information, and use this information to launch further attacks against the affected system.

CVE-2022-27189 CVSS:7.5

F5 BIG-IP is vulnerable to a denial of service, caused by a flaw when an Internet Content Adaptation Protocol (ICAP) profile is configured on a virtual server. By sending a specially-crafted traffic, a remote attacker could exploit this vulnerability to cause the Traffic Management Microkernel (TMM) memory resource utilization to increase, and results in a denial of service condition

CVE-2022-27230 CVSS:7.5

F5 BIG-IP Guided Configuration and APM are vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

CVE-2022-28691 CVSS:7.5

F5 BIG-IP is vulnerable to a denial of service, caused by a flaw when a Real Time Streaming Protocol (RTSP) profile is configured on a virtual server. By sending a specially-crafted traffic, a remote attacker could exploit this vulnerability to cause the Traffic Management Microkernel (TMM) memory resource utilization to increase, and results in a denial of service condition.

CVE-2022-28705 CVSS:7.5

F5 BIG-IP is vulnerable to a denial of service, caused by a flaw when an ePVA and the pva.fwdaccel BigDB variable enabled. By sending specially-crafted requests, a remote attacker could exploit this vulnerability to cause the Traffic Management Microkernel (TMM) process to terminate, and results in a denial of service condition

CVE-2022-28716 CVSS:7.5

F5 BIG-IP (AFM, CGNAT, PEM) are vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

CVE-2022-29491 CVSS:7.5

F5 BIG-IP (LTM, Advanced WAF, ASM, APM) are vulnerable to a denial of service, caused by a flaw when a virtual server is configured with HTTP, TCP on one side, and DTLS on the other. By sending specially-crafted requests, a remote attacker could exploit this vulnerability to cause the Traffic Management Microkernel (TMM) process to terminate, and results in a denial of service condition.

CVE-2022-26372 CVSS:7.5

F5 BIG-IP is vulnerable to a denial of service, caused by a flaw when a DNS listener is configured on a virtual server with DNS queueing. By sending specially-crafted requests, a remote attacker could exploit this vulnerability to cause an increase in memory resource utilization, and results in a denial of service condition.

CVE-2022-26415 CVSS:7.7

F5 BIG-IP could allow a remote authenticated attacker to bypass security restrictions, caused by a flaw in an undisclosed iControl REST endpoint. By sending a specially-crafted request, an attacker could exploit this vulnerability to bypass Appliance mode restrictions.

CVE-2022-27806 CVSS:8.7

F5 BIG-IP could allow a remote authenticated attacker to bypass security restrictions, caused by a command injection flaw in undisclosed URIs. By sending a specially-crafted request, an attacker could exploit this vulnerability to bypass Appliance mode restrictions.

CVE-2022-28707 CVSS:8

F5 BIG-IP is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote authenticated attacker could exploit this vulnerability to inject malicious script into a Web page which would be executed in a victim's Web browser within the security context of the hosting Web site, once the page is viewed. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

CVE-2022-29263 CVSS:7.8

F5 BIG-IP APM and APM Clients could allow a local authenticated attacker to gain elevated privileges on the system, caused not using best practice for saving temporary files by the Client Component Installer Service. By sending a specially-crafted request, an authenticated attacker could exploit this vulnerability to gain elevated privileges.

CVE-2022-1388 CVSS:9.8

F5 BIG-IP could allow a remote attacker to execute arbitrary commands on the system, caused by improper input validation. By sending specially-crafted requests to the management port and/or self IP addresses, an attacker could exploit this vulnerability to execute arbitrary commands, create or delete files, or disable services on the system.

Impact

- Security Bypass
- Information Disclosure
- Denial of Service
- Cross-Site Scripting
- Privilege Escalation

Indicators Of Compromise

CVE

- CVE-2022-25946
- CVE-2022-25990
- CVE-2022-27189
- CVE-2022-27230
- CVE-2022-28691
- CVE-2022-28705
- CVE-2022-29491
- CVE-2022-26372
- CVE-2022-26415
- CVE-2022-27806

- CVE-2022-28707
- CVE-2022-29263
- CVE-2022-1388

Affected Vendors

- F5

Affected Products

- F5 BIG-IP (APM) 14.1.0
- F5 BIG-IP (ASM) 14.1.0
- F5 BIG-IP (APM) 15.1.0
- F5 BIG-IP (ASM) 15.1.0
- F5 F5OS-A 1.0.0
- F5 BIG-IP 11.6.1
- F5 BIG-IP 13.1.0
- F5 BIG-IP 14.1.0
- F5 BIG-IP 11.6.5
- F5 BIG-IP (APM) 14.1.4
- F5 BIG-IP (APM) 16.1.0
- F5 BIG-IP 15.1.0
- F5 BIG-IP 14.1.4
- F5 BIG-IP (AFM) 15.1.0
- F5 BIG-IP (PEM) 15.1.0
- F5 BIG-IP (PEM) 14.1.0
- F5 BIG-IP (PEM) 13.1.0
- F5 BIG-IP (APM) 12.1.0
- F5 BIG-IP (APM) 13.1.0
- F5 BIG-IP 12.1.0
- F5 BIG-IP APM Clients 7.1.8

Remediation

Refer to F5 Security Advisory for patch, upgrade or suggested workaround information.

CVE-2022-25946 CVE-2022-25990 CVE-2022-27189 CVE-2022-27230 CVE-2022-28691 CVE-2022-28705 CVE-2022-29491 CVE-2022-26372 CVE-2022-26415 CVE-2022-27806 CVE-2022-28707 CVE-2022-29263 CVE-2022-1388