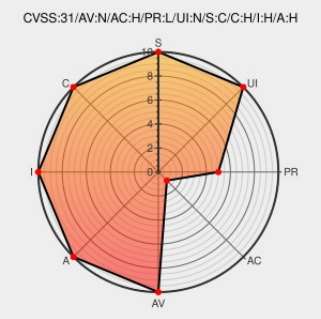
CVE-2023-22374

Published on: Not Yet Published

Last Modified on: 10/04/2023 04:55:00 PM UTC

CVE-2023-22374

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Big-ip Access Policy Manager from F5 contain the following vulnerability:

A format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

CVE-2023-22374 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **F5** - **BIG-IP** version **not down converted**

CVSS3 Score: 8.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
myF5	my.f5.com text/html	MISC my.f5.com/manage/s/article/K000130415

Related QID Numbers

377959 F5 BIG-IP IControl SOAP Vulnerability CVE-2023-22374 (K35253541)

Exploit/POC from Github

In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a forma…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Big-ip Access Policy Manager	13.1.5	All	All	All
Application	F5	Big-ip Access Policy Manager	17.0.0	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	13.1.5	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	17.0.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Analytics	13.1.5	All	All	All
Application	F5	Big-ip Analytics	17.0.0	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	13.1.5	All	All	All
Application	F5	Big-ip Application Acceleration Manager	17.0.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	13.1.0	All	All	All
Application	F5	Big-ip Application Security Manager	17.0.0	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	13.1.5	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	All	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	All	All	All	All

Application	F5	Big-ip Ddos Hybrid Defender	All	All	All	All
Application	F5	Big-ip Domain Name System	17.0.0	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	13.1.5	All	All	All
Application	F5	Big-ip Fraud Protection Service	17.0.0	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Link Controller	13.1.5	All	All	All
Application	F5	Big-ip Link Controller	17.0.0	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	13.1.5	All	All	All
Application	F5	Big-ip Local Traffic Manager	17.0.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	13.1.5	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	17.0.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Ssl Orchestrator	13.1.5	All	All	All
Application	F5	Big-ip Ssl Orchestrator	17.0.0	All	All	All
Application	F5	Big-ip Ssl Orchestrator	All	All	All	All
Application	F5	Big-ip Ssl Orchestrator	All	All	All	All
Application	F5	Big-ip Ssl Orchestrator	All	All	All	All

cpe:2.3:a:f5:big-ip_access_policy_manager:13.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager:17.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_firewall_manager:13.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_firewall_manager:17.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_analytics:13.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_analytics:17.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_analytics:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_analytics:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_analytics:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_acceleration_manager:13.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_acceleration_manager:17.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_acceleration_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_acceleration_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:13.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:17.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_ddos_hybrid_defender:13.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_ddos_hybrid_defender:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_ddos_hybrid_defender:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_ddos_hybrid_defender:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_domain_name_system:17.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_domain_name_system:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_domain_name_system:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_domain_name_system:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_fraud_protection_service:13.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_fraud_protection_service:17.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_fraud_protection_service:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_fraud_protection_service:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_link_controller:13.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_link_controller:17.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_link_controller:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_link_controller:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_link_controller:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_local_traffic_manager:13.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_local_traffic_manager:17.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_local_traffic_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_local_traffic_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_local_traffic_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_policy_enforcement_manager:13.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_policy_enforcement_manager:17.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_policy_enforcement_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_policy_enforcement_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_policy_enforcement_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_ssl_orchestrator:13.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_ssl_orchestrator:17.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_ssl_orchestrator:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_ssl_orchestrator:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_ssl_orchestrator:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@AcooEdi	CVE-2023-22374: F5 BIG-IP Format String Vulnerability dlvr.it/ShnFg4 via Rapid7 Blog https://t.co/rddP2emm7E	2023-02-01 16:00:05
@StopMalvertisin	Rapid7 Blog | CVE-2023-22374: F5 BIG-IP Format String Vulnerability stpmvt.com/40hQ6gt	2023-02-01 16:00:37

@CVEreport	CVE-2023-22374 : In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respectiv… twitter.com/i/web/status/1…	2023-02-01 18:09:33
/r/netcve	CVE-2023-22374	2023-02-01 18:40:22

← Previous ID

Next ID→