ZAFİYET BÜLTENİ

1 KASIM 2023

F5 BIG-IP

YAPILANDIRMA YARDIMCI PROGRAMINI ETKİLEYEN İKİ GÜVENLİK AÇIĞI YAYINLANDI

CVE: CVE-2023-46747
CVSS PUANI: 9.8
BAŞLIK: F5 BIG-IP YAPILANDIRMA YARDIMCI PROGRAMI KİMLİK DOĞRULAMA BYPASS GÜVENLİK AÇIĞI

CVE: CVE-2023-46748
CVSS PUANI: 8.8
BAŞLIK: F5 BIG-IP YAPILANDIRMA YARDIMCI PROGRAMI SQL ENJEKSİYONU GÜVENLİK AÇIĞI

ETKİLENEN SÜRÜMLER:

Ürün	Güvenlik Açığı Olduğu Bilinen Sürümler	Düzeltmeler
BIG-IP (tüm modüller)	17.1.0 - 17.1.1	17.1.0.3 + Hotfix-BIGIP-17.1.0.3.0.75.4-ENG 17.1.1 + Hotfix (Pending release)
	16.1.0 - 16.1.4	16.1.4.1 + Hotfix-BIGIP-16.1.4.1.0.50.5-ENG
	15.1.0 - 15.1.10	15.1.10.2 + Hotfix -BIGIP-15.1.10.2.0.44.2-ENG
	14.1.0 - 14.1.5	14.1.5.6 + Hotfix-BIGIP-14.1.5.6.0.10.6-ENG
	13.1.0 - 13.1.5	13.1.5.1 + Hotfix-BIGIP-13.1.5.1.0.20.2-ENG

REFERANSLAR:

https://www.picussecurity.com/resource/blog/cve-2023-46747-f5-big-ip-unauthenticated-remote-code-execution-vulnerability
https://my.f5.com/manage/s/article/K000137353
https://www.tenable.com/blog/cve-2023-46747-critical-authentication-bypass-vulnerability-in-f5-big-ip

CVE-2023-46747 - F5 BIG-IP Yapılandırma Yardımcı Programı Kimlik Doğrulama Bypass Güvenlik Açığı

Açıklama:
Yapılandırma Yardımcı Programı olarak da adlandırılan F5 Trafik Yönetimi Kullanıcı Arayüzü (TMUI) kullanıcılara BIG-IP sisteminin birçok işlevini yönetmek ve izlemek için sezgisel bir platform sağlayan bir grafik kullanıcı arayüzü (GUI) görevi görür. F5 TMUI, tüm HTTP isteklerini arka uçtaki farklı hizmetlere yönlendirir ve "/tmui" uç noktalarına yönelik istekler, 8009 numaralı bağlantı noktasını dinleyen Apache JServ Protokolü (AJP) hizmetine iletilir. "/tmui" uç noktasında, yönetim bağlantı noktası ve/veya kendi IP adresleri aracılığıyla BIG-IP sistemine ağ erişimi olan, kimliği doğrulanmamış bir saldırganın root yetkisiyle rastgele sistem komutları yürütmesine izin verebilen güvenlik açığı keşfedilmiştir.

Geçici Hafifletme Yöntemi:
Bu zafiyet Trafik Yönetimi Kullanıcı Arayüzü'nün (TMUI) internette kullanıma sunulması durumunda kullanılabilir. Bu nedenle, Yapılandırma yardımcı programına erişimin yalnızca güvenilir ağlara veya cihazlara veya belirli IP aralıklarına kısıtlanmasıyla kötüye kullanım riski geçici olarak azaltılabilir.

CVE-2023-46748 - F5 BIG-IP Yapılandırma Yardımcı Programı SQL Enjeksiyonu Güvenlik Açığı

Açıklama:

CVE-2023-46748, BIG-IP Yapılandırma Yardımcı Programında yüksek önem derecesine sahip, kimliği doğrulanmış bir SQL injection güvenlik açığıdır. SQL enjeksiyon kusuru, Kimliği doğrulanmış bir saldırganın, BIG-IP yönetim bağlantı noktası ve/veya kendi IP adresleri aracılığıyla, Yapılandırma yardımcı programına ağ erişimiyle rastgele sistem komutlarını yürütmesine olanak tanır.
Tehdit aktörlerinin bu güvenlik açığını CVE-2023-46747 ile birlikte kullandığını gözlemlendi. Aşağıda CVE-2023-46748 ile gözlemlenen PoC verilmiştir.

/var/log/tomcat/catalina.out dosyası incelendiğinde:
{...}
java.sql.SQLException: Column not found: 0.
{...)
sh: no job control in this shell
sh-4.2$ <EXECUTED SHELL COMMAND>
sh-4.2$ exit.

örneğinde aşağıdakilere dikkat edilmeli:

Column not found: 0 satırında, 0 farklı bir sayı ile değiştirilebilir.
<EXECUTED SHELL COMMAND> satırında, komut farklı bir komutla değiştirilecektir.

Geçici Hafifletme Yöntemi:

Bu zafiyet Yapılandırma Yardımcı Programı olarak da adlandırılan Trafik Yönetimi Kullanıcı Arayüzü'nün (TMUI) internette kullanıma sunulması durumunda kullanılabilir. Bu nedenle, Yapılandırma yardımcı programına erişimin yalnızca güvenilir ağlara veya cihazlara veya belirli IP aralıklarına kısıtlanmasıyla kötüye kullanım riski geçici olarak azaltılabilir.