FortiSIEM

Uzaktan Kimliği Doğrulanmamış OS Komutu Enjeksiyonu

CVE: CVE-2023-34992

CVSS Puanı: 9.7

Etkilenen Ürünler:

FortiSIEM sürüm 7.0.0
FortiSIEM sürüm 6.7.0 ila 6.7.5
FortiSIEM sürüm 6.6.0 ila 6.6.3
FortiSIEM sürüm 6.5.0 ila 6.5.1
FortiSIEM sürüm 6.4.0 ila 6.4.2

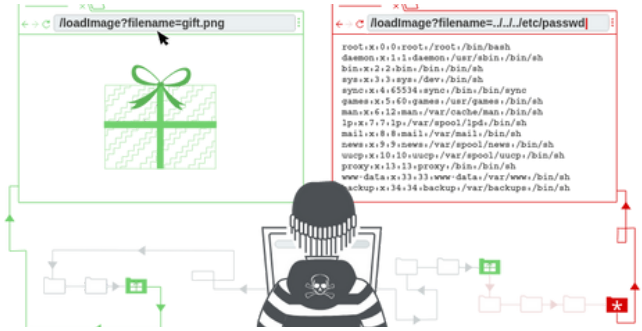
Çözümler:

FortiSIEM sürüm 7.0.1 veya üstüne yükseltin.
FortiSIEM sürüm 6.7.6 veya üstüne yükseltin.
FortiSIEM'in gelecek 6.6.4 veya üzeri sürümüne yükseltin.
FortiSIEM'in gelecek 6.5.2 veya üzeri sürümüne yükseltin.
FortiSIEM'in gelecek 6.4.3 veya üzeri sürümüne yükseltin.

Açıklama:

FortiSIEM, Fortinet tarafından geliştirilen bir güvenlik bilgi ve olay yönetimi (SIEM) çözümüdür.
CVE-2023-34992, FortiSIEM'de bir os komutunda kullanılan özel öğelerin uygunsuz şekilde etkisizleştirilmesiyle, kimliği doğrulanmamış uzak bir saldırganın hazırlanmış API istekleri aracılığıyla yetkisiz komutlar yürütmesine izin verebilen güvenlik açığıdır.

Referans: https://www.fortiguard.com/psirt/FG-IR-23-130



Çoklu Path Traversal Güvenlik Açığı

CVE: CVE-2023-40714

CVSS Puanı: 9.7

Etkilenen Ürünler:

FortiSIEM sürüm 7.0.0
FortiSIEM sürüm 6.7.0 ila 6.7.3
FortiSIEM sürüm 6.6.0 ila 6.6.3
FortiSIEM sürüm 6.5.0 ila 6.5.1
FortiSIEM sürüm 6.4.0 ila 6.4.2

Çözümler:

FortiSIEM sürüm 7.0.1 veya üstüne yükseltin.
FortiSIEM sürüm 6.7.4 veya üstüne yükseltin.
FortiSIEM sürüm 6.6.4 veya üstüne yükseltin.
FortiSIEM sürüm 6.5.2 veya üstüne yükseltin.
FortiSIEM sürüm 6.4.3 veya üstüne yükseltin.

Açıklama:

FortiSIEM, Fortinet tarafından geliştirilen bir güvenlik bilgi ve olay yönetimi (SIEM) çözümüdür.
CVE-2023-40714, FortiSIEM dosya yükleme bileşenlerinde kritik önem sahip bir güvenlik açığıdır. FortiSIEM GUI'sinin kimliği doğrulanmış, düşük ayrıcalıklı bir kullanıcısının ayrıcalıklarını yükseltmesine ve özel olarak hazırlanmış HTTP istekleri aracılığıyla temel dosya sistemindeki rastgele dosyaları değiştirmesine olanak tanıyan bir relative path traversal güvenlik açığıdır.

Referans: https://www.fortiguard.com/psirt/FG-IR-23-085