CVE-2022-22963-22965 Güvenlik Açığı Bilgilendirmesi

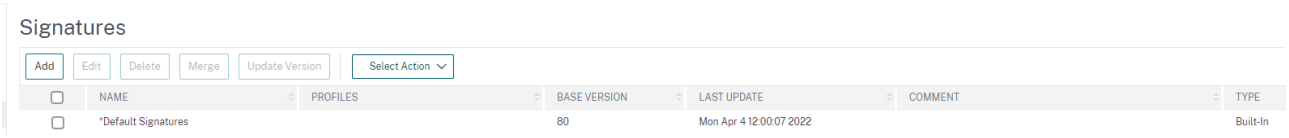
Spring Framework (5.3.0 to 5.3.17, 5.2.0 to 5.2.19 ve daha eski sürümler) versiyonlarını etkileyen bir güvenlik açığı çıkmıştır.Bu güvenlik açığına karşı Citrix ADC üzerinde çalışan Spring Fremework kullanan servislerinizi korumak için WAF imza sürümünü 80 versiyona güncellemeli ve 999004, 999005 ID numaralı imzalar blok mode da aktif edilmelidir.İmzaya alternatif olarak citrix policy ile servis veya global policy bind tanımı yaparak güvenlik açığına karşı koruma sağlayalabilirsiniz.Açık ile ilgili daha detaylı bilgi ve destek almak için citrix_tr@exclusive-networks.com adresine mail atabilirsiniz.

https://www.citrix.com/blogs/2022/04/01/guidance-for-reducing-spring4shell-security-vulnerability-risk-with-citrix-waf/

WAF Policy İmza Koruması ;

ENABLED	BLOCK	LOG	STATS	ID	LOGSTRING	CATEGORY	SOURCE	SOURCE-ID	CPU USAGE	YEAR	SEVERITY
✓	✓	✓	×	999005	WEB-MISC Spring Cloud Function - Code Injection Vulnerability (CVE-2022-22963)	web-misc	Citrix	999005	LOW	2022	MEDIUM

ENABLED	BLOCK	LOG	STATS	ID	LOGSTRING	CATEGORY	SOURCE	SOURCE-ID	CPU USAGE	YEAR	SEVERITY
✓	✓	✓	×	999004	WEB-MISC Spring4Shell Spring Core Framework - RCE Vulnerability (CVE-2022-22965)	web-misc	Citrix	999004	MEDIUM	2022	MEDIUM



Citrix Policy :

add responder policy mitigate_cve_2022_22963_22965 q^(HTTP.REQ.FULL_HEADER.SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.CONTAINS("spring.cloud.function.routing-expression") || HTTP.REQ.BODY(8192).SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.CONTAINS(".classLoader"))^ DROP