CVE-2021-44228 Güvenlik Açığı Bilgilendirmesi

Apache Log4j Java tabanlı uygulamaları etkileyen kritik bir güvenlik açığı çıkmıştır.Citrix yayımlamış olduğu makalede Citrix cihazlarının bu güvenlik açığından etkilenmediğini bildirmiştir.Bu açığa karşı Citrix üzerinde yer alan servislerinizi korumaak için WAF imza sürümünüz 72 güncelleyerek 999077,999078,999079,999080 ID numaralı imzaları aktif edebilirsiniz.İmzaya alternatif olarak koruma sağlamak istediğiniz servisleriniz üzerinde appfw policy bind edilebilir.Açık ile ilgili daha detaylı bilgi ve yardım almak için citrix_tr@exclusive-networks.com adresine mail atabilirsiniz.

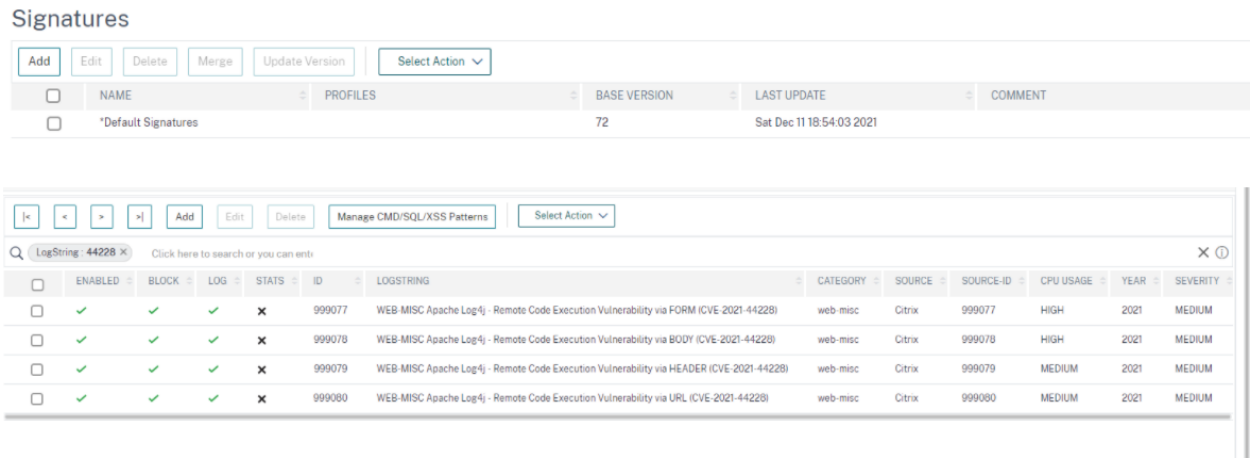
https://support.citrix.com/article/CTX335705

Citrix Security Advisory for Apache CVE-2021-44228

Citrix is closely monitoring the recent vulnerability disclosure by Apache Software Foundation on December 10th, 2 CVE-2021-44228. Citrix has mobilized its Security and IT organizations to investigate the issue and immediately mitiga potential risks.

support.citrix.com

WAF Policy İmza Koruması:



APPFW Policy :

```
add appfw policy cve-2021-44228_pol
"HTTP.REQ.FULL_HEADER.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"jndi:ldap\") ||
HTTP.REQ.FULL_HEADER.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"jndi:ldaps\") ||
HTTP.REQ.FULL_HEADER.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"jndi:rmi\") ||
HTTP.REQ.FULL_HEADER.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"jndi:dns\") ||
HTTP.REQ.FULL_HEADER.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"jndi:${lower:\") ||
HTTP.REQ.FULL_HEADER.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"${${::-j\") ||
HTTP.REQ.FULL_HEADER.SET_TEXT_MODE(IGNORECASE).CONTAINS(\":-j}ndi\") ||
HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"jndi:ldap\") ||
HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"jndi:ldaps\") ||
HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"jndi:rmi\") ||
HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"jndi:dns\") ||
HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"jndi:${lower:\") ||
HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"${${::-j\") ||
HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS(\":-j}ndi\") ||
HTTP.REQ.BODY(50000).SET_TEXT_MODE(IGNORECASE).CONTAINS(\"jndi:ldap\") ||
HTTP.REQ.BODY(50000).SET_TEXT_MODE(IGNORECASE).CONTAINS(\"jndi:ldaps\") ||
HTTP.REQ.BODY(50000).SET_TEXT_MODE(IGNORECASE).CONTAINS(\"jndi:rmi\") ||
HTTP.REQ.BODY(50000).SET_TEXT_MODE(IGNORECASE).CONTAINS(\"jndi:dns\") ||
HTTP.REQ.BODY(50000).SET_TEXT_MODE(IGNORECASE).CONTAINS(\"jndi:${lower:\") ||
HTTP.REQ.BODY(50000).SET_TEXT_MODE(IGNORECASE).CONTAINS(\"${${::-j\") ||
HTTP.REQ.BODY(50000).SET_TEXT_MODE(IGNORECASE).CONTAINS(\":-j}ndi\")" APPFW_BLOCK
```