

heimdall

security research

A DIVISION OF ISH

heimdall
security research



Ransomware Royal explora a Vulnerabilidade Citrix (CVE-2022-27510) para seus ataques

Receba alertas e informações sobre segurança cibernética rapidamente, por meio do nosso Twitter:

https://twitter.com/heimdallish













índice

1 SOBRE A EXPLORAÇÃO 5
2 COMO ESTÁ OCORRENDO A EXPLORAÇÃO DA VULNERABILIDADE? 6
3 MITIGAÇÃO 7
4 REFERÊNCIAS 8

1 SOBRE A EXPLORAÇÃO

Recentemente a empresa At-bay publicou um estudo relacionado ao *Ransomware* Royal no qual afirma que os operadores estão explorando a vulnerabilidade Citrix (CVE-2022-27510) para obter controle dos sistemas e lançar o ataque.

A vulnerabilidade mencionada foi anunciada em 8 de novembro de 2022 pela Citrix, que afirmou que seria uma falha crítica de segurança, pois permite o possível desvio de medidas de autenticação em dois produtos Citrix: o *Application Delivery Controller* (ADC) e o *Gateway*.

2 COMO ESTÁ OCORRENDO A EXPLORAÇÃO DA VULNERABILIDADE?

A exploração da referida vulnerabilidade está de acordo com a de vulnerabilidades semelhantes que foram vistas no passado, sendo que o Royal está explorando essa uma de **desvio de autenticação** em produtos Citrix para obter acesso não autorizado a dispositivos com Citrix ADC ou Citrix *Gateway* e lançar o ataque *ransomware*.

Além do método de exploração, existe a descrição dos produtos Citrix que são afetados, uma vez que, que devido à grande variedade de produtos para virtualização, rede e computação em nuvem, as versões Citrix ADC e Citrix *Gateway* são afetadas pela vulnerabilidade de desvio de autenticação remota (CVE-2022-27510):

Product	Affected Versions	Fixed Versions
Citrix ADC and Citrix Gateway 13.1	Before 13.1-33.47	13.1-33.47 and later
Citrix ADC and Citrix Gateway 13.0	Before 13.0-88.12	13.0-88.12 and later
Citrix ADC and Citrix Gateway 12.1	Before 12.1-65.21	12.1-65.21 and later
Citrix ADC 12.1-FIPS	Before 12.1-55.289	12.1-55.289 and later

Figura 1. Descrição do produto, versões afetadas e versões de correção apresentadas pela At-bay.

3 MITIGAÇÃO

Recomendamos que as organizações afetadas pela vulnerabilidade do Citrix ADC e Citrix *Gateway* **instalem as versões atualizadas o mais rápido possível**, visando mitigá-la.

Até o presente momento não foi possível identificar uma POC ou até mesmo se a exploração via *exploit* está disponível para a verificação de *logs* pelo público.

Por fim, recomendamos que seja constantemente realizada a varredura nos produtos utilizados, a fim de identificar vulnerabilidades existentes para aplicação de *patches* ou atualizações de segurança, caso haja a disponibilidade destes.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Publicação *Royal Ransomware – At-Bay*
- CVE-2022-27510 - Citrix


heimdall
security research
A DIVISION OF ISH