Prezado cliente,

A **Logical IT** alerta para a publicação de uma nova vulnerabilidade crítica, remotamente explorável no software ***VMware Cloud Director***.

O ***VMware Cloud Director 10.0.x*** antes da versão **10.0.0.2**, **9.7.0.x** antes da versão **9.7.0.5**, **9.5.0.x** antes da versão **9.5.0.6** e **9.1.0.x** antes da versão **9.1.0.4**. Possui uma fragilidade pois não tratam corretamente certos tipos de requisições remotas. Esta condição leva a fragilidade de exploração remota através da injeção de código malicioso.

Um **atacante autenticado** pode enviar um script remoto ao ***VMware Cloud Director***, ocasionando na execução arbitrária de comandos. Em um cenário hipotético pode ocasionar na alteração remota de uma senha administrativa, elevando um usuário comum para privilégios de administrador do ***VMware Cloud Director.***

Essa vulnerabilidade pode ser explorada **por meio de interfaces de usuário baseadas em HTML5 e Flex, na interface do API Explorer e no acesso à API**.
Nosso time reforça que foram publicados scripts para provar o conceito de exploração da vulnerabilidade. Estes scripts estão disponíveis na Internet para download.

Lista de Vulnerabilidades Críticas

- **CVE-2020-3956** - VMware Director Remote Code Execution

Sistemas Afetados

- **VMware Cloud Director** (anteriormente conhecido como ***vCloud Director***)

Vulnerabilidades Publicadas					
Identificação da Vulnerabilidades MITRE (CVE)	**Explorável Remoto?**	**Impacto**	**Divulgado Publicamente?**	**Exploração Disponível?**	**Pontuação de Severidade (CVSS)**
CVE-2020-3956	Sim	Remote Code Execution	Sim	Sim	**8.8**

Serviço de Gestão de Vulnerabilidades		
Identificação da Vulnerabilidades MITRE (CVE)	**Nome da Assinatura**	**Data de Publicação**
CVE-2020-3956	Em desenvolvimento	**N/I**

MSS/SOC (Content Security)					
Identificação da Vulnerabilidades MITRE (CVE)	**Soluções: Trend Micro (Módulo: Virtual Patch)**				
	Deep Security	**Apex One**	**Vulnerability Protection (VP)**	**Tipping Point**	**Data da Última Atualização**
	Nome da Assinatura				
CVE-2020-2798	Em análise	**N/A**	**N/A**	Em análise	**N/I**

Recomendação para solução definitiva

Recomendamos que sejam aplicadas se possível as correções disponibilizadas pela VMware descritas no link do seu artigo de correção.

Workarounds e Fatores de Mitigação

Medidas Preventivas:

- Restringir o acesso remoto administrativo ao servidor / appliance com ***VMware Cloud Director*** somente para os endereços de rede dos usuários administradores comuns;
- Monitoramento do uso e alteração de senhas de contas administrativas;
- Executar o monitoramento de códigos maliciosos através de soluções com tecnologia de virtual patch;

Adicionalmente a VMWARE documentou possíveis medidas alternativas neste link em sua matriz de solução e workaround.

Como a LIT suporta nossos clientes para endereçar o risco destas ameaças no ambiente dos nossos clientes.

Nossos especialistas **coordenarão em paralelo com nossos clientes** um plano para implementação das ações de identificação, detecção e proteção planejadas para controlar o risco de potenciais explorações desta ameaça.

- **Identificação da Fragilidade (Gestão de Vulnerabilidades);**

Através do nosso serviço de Gestão de Vulnerabilidades agimos proativamente executando varreduras planejadas com os nossos clientes para identificações específicas para as fragilidades reportadas.

- **Detecção de Ameaças (SOC);**

O Nosso serviço do Centro de Operações de Segurança usa da base de Inteligência de Ameaças e Base de Conhecimento de comportamento para criar alertas personalizados para detectar e caçar explorações de ameaças, suportando agilidade na resposta e redução de impactos potenciais.

- **Proteção de Explorações (MSS);**

Nosso time de MSS trabalhará assim que disponível no planejamento e Implementação de Bloqueio das Ameaças **remotamente exploráveis** através das soluções com a tecnologia de **virtual patch** para as vulnerabilidades consideradas como remotamente exploráveis.

O Time da Logical IT está à disposição para mais esclarecimentos.

Informações adicionais (Ref.):

https://citadelo.com/en/blog/full-infrastructure-takeover-of-vmware-cloud-director-CVE-2020-3956/
http://packetstormsecurity.com/files/157909/vCloud-Director-9.7.0.15498291-Remote-Code-Execution.html
https://citadelo.com/en/blog/full-infrastructure-takeover-of-vmware-cloud-director-CVE-2020-3956/
https://github.com/aaronsvk/CVE-2020-3956
https://www.vmware.com/security/advisories/VMSA-2020-0010.html