Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Alerta de Segurança 005/2020 - Cogetic

Em 6 de novembro de 2020

Para: Gestores de TI das unidades da Fiocruz

Assunto: Vulnerabilidades críticas em múltiplas plataformas

Prezados Gestores de TI,

Nos últimos dias temos recebidos notícias de ataques à infraestrutura de órgãos do governo e com incidentes relacionados à *Ransomware*. Conforme Alertas de Segurança emitidos pela Rede Nacional de Ensino e Pesquisa – RNP e pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR Gov estão sendo exploradas vulnerabilidades críticas em múltiplas plataformas sabidamente utilizadas de forma ampla em diversas organizações, cuja exploração pode resultar na execução de códigos remotos, infecção por *ransomwares*, entre outros incidentes graves.

As vulnerabilidades estão associadas principalmente à plataforma de virtualização VMWare (CVE-2020-3992 e CVE-2019-5544) e a sistemas operacionais Microsoft Windows (CVE-2020-1472). No caso do VMWare a vulnerabilidade se refere à execução remota de código e no Windows a elevação de privilégio.

Estas vulnerabilidades não são recentes e estão sendo usados por hackers para exploração de forma maliciosa. Recomendamos a atualização dos Sistemas Operacionais Windows (servidores e desktops) e aplicações VMWare, com os hotfix e patches adequados distribuído pelo fabricante.

Recomendações gerais:

- Os *endpoints* devem estar protegidos com soluções anti-malware atualizado, e com recursos de detecção e combate a *ransomware*;
- O módulo de IPS deve estar habilitado nas soluções de Firewall e do Deep Security (observar que o modo Prevent deve estar habilitado), verificando se existe assinatura específica para a CVE-2020-1472;
- Monitorar e investigar qualquer host com tráfego muito elevado para a internet;
- Desabilitar regras de acesso ANY para HTTP e HTTPS para internet;

- Não permitir acesso à internet, com destinos não especificados e com reputação comprometida.
- Bloquear arquivos com as seguintes assinaturas:
    - MD5 (svc-new/svc-new) = 4bb2f87100fca40bfbb102e48ef43e65
    - MD5 (notepad.exe) = 80cfb7904e934182d512daa4fe0abbfb
    - SHA1 (notepad.exe) = 9df15f471083698b818575c381e49c914dee69de
    - SHA1 (svc-new/svc-new) = 3bf79cc3ed82edd6bfe1950b7612a20853e28b09
- Revisar e restringir (temporariamente) a permissão dos Administradores do AD (Active Directory);
- Verificar usuários "logados" no AD, efetuar o *sign out* destes usuários;
- Avaliar a necessidade de alterar a permissão dos compartilhamentos de rede (momentaneamente) para SOMENTE LEITURA, (não vai parar o serviço e evita perda de dados, e disseminação);
- Caso os servidores possuam usuários locais configurados, desabilitá-los ou alterar a senha utilizadas por eles;
- Desabilitar o CIM Server no VMware ESXi: https://kb.vmware.com/s/article/76372
- Fortalecer a inspeção de e-mails nas ferramentas de relay e antispam.
- Adotar a lista de reputação de IP's mantida pelo SERPRO, onde constam endereços maliciosos envolvidos em ataques a sites do governo: http://reputation.serpro.gov.br/
- Manter estações de trabalho com antivírus instalado e atualizado.
- Bloquear imediatamente arquivos com as seguintes assinaturas:
    - MD5 (svc-new/svc-new) = 4bb2f87100fca40bfbb102e48ef43e65
    - MD5 (notepad.exe) = 80cfb7904e934182d512daa4fe0abbfb
    - SHA1 (notepad.exe) = 9df15f471083698b818575c381e49c914dee69de
    - SHA1 (svc-new/svc-new) = 3bf79cc3ed82edd6bfe1950b7612a20853e28b09
- Manter o sistema operacional de servidores e estações de trabalho atualizados;

- Analisar continuamente relatório das plataformas *antimalware*;
- Ativar filtro web e bloquear acesso à internet para conteúdo não classificado.
- Ativar controle de reputação web;
- Habilitar 2FA para autenticação em ativos críticos.
- Aplicar privilégios mínimos no AD;
- Desabilitar conta *Guest*;
- Segregar as contas de administração e administração de domínio;
- Criar GPO para efetuar o *logoff* de usuários, por inatividade no AD em vez de *disconnect*.
- Auditar contas administrativas de Domínio.
- Revisar as políticas de backups dos principais sistemas, inclusive testar uma amostragem de backup e garantir que a restauração está em conformidade.
- Revisar acessos privilegiados em todas as consoles de gerência (Firewall, IPS, Anti-DDoS, Filtro de Conteúdo, Virtualizadores e ativos de rede);
- Verificar e apagar contas que não são utilizadas nos ativos.

Recomendações sobre monitoramento:

- Criação de "Arquivos Canário", com *checksum* monitorado por ferramenta de infraestrutura (Arquivos que seriam alterados apenas por um Ransomware, mas nunca por um administrador ou script de sistema).
- Monitorar assinaturas de IPS e logs (SIEM) para eventos suspeitos de tentativas de escalação de privilégio, como exemplo da CVE 2020-1472 e conexões TCP Netlogon suspeitas com origem em redes externas.
- Sugestão de regra Yara para encontrar variantes do malware. Os órgãos podem usar estes padrões de string como parâmetros de inspeção em seus controles:

```
rule RansomwareESXi
```

```
    {
            strings:
                    $string1 = "ransomware.c" nocase
                    $string2 = "cryptor.c" nocase
                    $string3 = "logic.c" nocase
                    $string4 = "enum_files.c" nocase
                    $string5 = "aes.c" nocase
                    $string6 = "rsa.c" nocase
                    $string7 = "crtstuff.c" nocase
                    $string8 = "mbedtls" nocase
            condition:
                    all of them
     }
rule BackdoorNotepad
{
       strings:
              $string1 = "c:\\windows\\INF\\config.dat" nocase
       condition:
              $string1
}
```

- Monitorar tentativas de acesso à porta 427 com destino a administração de virtualização;
- Monitorar bloqueio de contas no Active Directory ou LDAP por tentativa de login falhas (account lockout);
- Criar regra de monitoração de força bruta de autenticação em AD e autenticação Local. X tentativas falhas de login dentro intervalo Y / seg.
- Monitorar tentativas de acesso por meio de pass-the-hash - userName != “ANONYMOUS LOGON” - Microsoft-Windows-Security-Auditing = 4624 - Microsoft-Windows-Security-Auditing = 4625 - LogonProcessName = 'NtLmSsp'

Referência:

- https://www.rnp.br/arquivos/documents/CAIS_Alerta_Multiplas_vulnerabilidades_cr%c3%adticas_em_plataformas.txt?RP7ZfG4CJoaecXaf6nsVXeWUXr.ovKuq
- https://www.rnp.br/arquivos/documents/A%c3%a7%c3%b5es%20Ransomware.pdf?NGr_iXvKSTGP2O3F_j5QIEdssZEOiuZr
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472
- https://www.vmware.com/security/advisories/VMSA-2020-0023.html
- https://www.vmware.com/security/advisories/VMSA-2019-0022.html

Coordenação-Geral de Gestão de Tecnologia da Informação
Serviço de Segurança da Informação e Comunicações