Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal

Alerta nº 03/2016 – Distribuição de Ferramentas para Exploração de Vulnerabilidades em Equipamentos Cisco, Fortinet e WatchGuard

1. Descrição do Problema

Em 13 de agosto de 2016, um grupo intitulado *Shadow Brokers* disponibilizou um grupo de ferramentas para exploração de vulnerabilidades em equipamentos Cisco, Fortinet e WatchGuard. As ferramentas incluem ferramentas de exploração, de varredura e de estabelecimento de conexão e documentação.

2. Equipamentos Afetados

- Cisco ASA 8.4(3) e superiores
- Série Cisco ASA 5500
- Série de firewalls nova geração Cisco ASA 5500-X
- Módulo de serviços Cisco ASA para switch da série Cisco Catalyst 6500 e roteadores da série Cisco 7600
- Firewall para nuvem Cisco ASA 1000V
- Cisco Adaptive Security Virtual Appliance (ASAv)
- Série Cisco Firepower 4100
- Módulo de segurança Cisco Firepower 9300 ASA
- Software Cisco Firepower Threat Defense
- Cisco Industrial Security Appliance 3000
- Cisco PIX Firewalls*
- Cisco Firewall Services Module (FWSM)*
- FortiGate (FortiOS) 4.3.8 e anteriores
- FortiGate (FortiOS) 4.2.12 e anteriores
- FortiGate (FortiOS) 4.1.10 e anteriores
- FortiSwitch 3.4.2 e anteriores
- WatchGuard RapidStream

* Esses produtos já não são suportados pelo fabricante, atingiram o End-of-Life (EOL).

3. Possíveis Riscos

As ferramentas foram testadas por órgãos competentes e foi verificada a completa funcionalidade das mesmas e que permitem a um atacante remoto:

- Pular as fases de autenticação;
- Obter controle dos equipamentos com privilégio administrativo;
- Obter informações sensíveis como senhas de VPN e chaves criptográficas; e
- Escutar e adulterar o tráfego não criptografado que passe pelos equipamentos comprometidos.

4. Sugestões para Mitigação do Problema

- Verificar se sua organização possui algum dos equipamentos afetados listados e se não estão comprometidos;
- Se houver indícios de comprometimento:
  - Salvar os arquivos de configuração do equipamento;
  - Reinstalar uma versão nova e atualizada do sistema operacional do equipamento;
  - Reconfigurar o equipamento;
  - Aplicar as atualizações e os patches disponibilizados pelo fabricante, quando for o caso.
- Restringir as conexões SSH e Telnet aos equipamentos para somente poucos IP confiávies e somente quando for estritamente necessário;
- Habilitar multi-fator de autenticação, quando disponível;
- Seguir as orientações do fabricante quanto à configuração segura dos equipamentos;
- Planejar a substituição urgente de equipamentos não suportados pelo fabricante, que atingiram o End-Of-Life (EOL), para garantir que o equipamento receba atualizações, principalmente as de segurança.

5. Referências:

https://blogs.cisco.com/security/shadow-brokers
http://tools.cisco.com/security/center/viewErp.x?alertId=ERP-56516
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-cli
http://fortiguard.com/advisory/FG-IR-16-023
https://www.secplicity.org/2016/08/16/nsa-equation-group-exploit-leak-mean/
http://www.topsec.com.cn/aqtb/aqtb1/jjtg/160820.htm
http://www.huawei.com/en/psirt/security-notices/huawei-sn-20160823-01-shadowbrokers-en
https://forums.juniper.net/t5/Security-Incident-Response/Shadow-Brokers-Release-of-Hacking-Code/ba-p/296128
https://devcentral.f5.com/articles/leaked-shadowbrokers-tools-does-not-target-f5-networks-21700
https://musalbas.com/2016/08/16/equation-group-firewall-operations-catalogue.html
http://cert.europa.eu/static/SecurityAdvisories/CERT-EU-SA2016-133.pdf
https://www.cert.gov.uk/resources/advisories/advisory-multiple-vulnerabilities-in-various-products-posted-online/
https://xorcat.net/2016/08/16/equationgroup-tool-leak-extrabacon-demo/
https://xorcat.net/2016/08/19/equation-group-crashing-asas-follow-up/

Brasília, 01 de setembro de 2016.

Equipe do CTIR Gov