https://www.ctir.gov.br

29 de junho de 2019

Contato com o **CTIR Gov**

Informações:
https://www.ctir.gov.br

E-mail:
cgtir@presidencia.gov.br

Telefone:
+55 (61) 3411-2315

Alerta nº 03/2019 – *Malware Silex em dispositivos IoT*

Atualização: 29 de junho de 2019

Notificação de Incidentes:
ctir@ctir.gov.br

INOC-DBA: 10954*810

1. Descrição do Problema

Um novo tipo de *malware* está afetando dispositivos ligados à *Internet* das Coisas (*IoT*). Ele é nomeado como *Silex* e afeta dispositivos *IoT*, como roteadores e câmeras IP com serviço *telnet* (porta 23) em execução em sua interface voltada para a *Internet*.

O *malware* tenta obter acesso a dispositivos *IoT* usando credenciais de *telnet* padrão, que são amplamente usadas, e corrompe o *firmware* dos dispositivos que estão instalados com as credenciais de fábrica, estragando o armazenamento, eliminando as regras de *firewall* e as interfaces de rede, tornando-os inutilizáveis.

O CTIR Gov recomenda a divulgação, em todos os órgãos de governo e entidades vinculadas, do presente alerta, contendo orientações de recursos disponibilizados para a prevenção, verificação e mitigação de incidentes relacionados ao tema.

Outros alertas e recomendações podem ser encontrados em *https://www.ctir.gov.br/alertas/*

2. Impacto

Um dispositivo corrompido será inutilizável até que seu *firmware* seja reinstalado.

3. Dispositivos Afetados

Dispositivos IoT com:
• *Busybox* em execução;
• *Telnet* escutando na porta 23; e
• Credenciais padrão de fábrica.

4. Recomendações

As seguintes práticas são recomendadas para ajudar a proteger as redes contra essa ameaça:

- Alterar as credenciais padrão de fábrica do dispositivo;
- Usar *password/passphrase* longa e aleatória que inclua mistura de letras maiúsculas e minúsculas, números e símbolos.
- Bloquear a interface *telnet* voltada para a *Internet*.

5. Referências

- *[SingCERT] Alert on New Silex Malware on IoT Devices* - Disponível em: *https://www.csa.gov.sg/singcert/news/advisories-alerts/alert-on-new-silex-malware-on-iot-devices*. Acesso em: 27 de junho 2019.
- *New Silex malware is bricking IoT devices, has scary plans* - Disponível em: *https://www.zdnet.com/article/new-silex-malware-is-bricking-iot-devices-has-scary-plans/*. Acesso em: 27 de junho 2019.
- *Silex malware bricks thousands of IoT devices in a few hours* - Disponível em: *https://securityaffairs.co/wordpress/87609/iot/silex-malware-bricks-iot-devices.html*. Acesso em: 27 de junho 2019.

Coordenação-Geral do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CGCTIR)

Informações: cgtir@presidencia.gov.br
Notificação de incidentes: ctir@ctir.gov.br