Alerta de Segurança 001/2013 - CGTI/VPGDI

Em 29 de janeiro de 2013

A/C: Serviço de Infraestrutura Tecnológica, Serviço de Suporte ao Usuário; Outsourcing HP

Prezados,

No dia 28/1/2013 fomos notificados que algumas impressoras instaladas no prédio "bandejão" estavam realizando impressões não solicitadas. Após a coleta de algumas evidências observamos que a maioria das impressoras da rede 157.86.13.0/24 estão com a interface administrativa via web habilitadas e acessíveis tanto internamente quanto a partir da internet. Posteriormente identificamos que a rede 157.86.12 apresenta a mesma vulnerabilidade. Foi possível observar a possibilidade de envio de um documento diretamente para a uma impressora através do link http://[IP]/hp/device/this.LCDispatcher?nav=hp.Print.

Como forma de contenção dos eventos foi implementada uma restrição de acesso aos IPs das impressoras e estações da rede 157.86.13/24 através de regras de Firewall/ACL's. De forma complementar recomendamos que sejam implementadas as seguintes ações:

I. Restringir a interface administrativa das impressoras por login e senha somente para acesso pelo suporte da HP;
II. Verificação das demais redes sob responsabilidade da CGTI, implementando as restrições de acesso através do Firewall quando estas estiverem acessíveis externamente.
III. Atualização do sistema operacional das estações, substituindo o Windows XP pela versão mais recente, incluindo todas as atualizações de segurança (*Service Packs* e *Patches*).
IV. Integração dos usuários de impressão com o controlador de domínio, evitando impressões anônimas ou remotas sem autenticação.

Fundação Oswaldo Cruz – FIOCRUZ – Coordenação de Gestão de TI - Av. Brasil, 4.365 – Manguinhos, RJ. CEP: 21040-360
Castelo Mourisco, sala 105. Tel.: 3885-1724 Site: http://cgti.fiocruz.br