Smartphones Google Nexus são vulneráveis a ataques DDoS via SMS
Lucian Constantin

Crackers podem forçar os dispositivos a reiniciar ou a não se conectar à Internet móvel por meio do envio de um grande número de mensagens SMS especiais.
Ciberciminosos poderiam forçar os smartphones da linha Nexus do Google a reiniciarem ou a não se conectarem à Internet móvel por meio do envio de um grande número de mensagens SMS especiais.

O problema foi identificado por Bogdan Alecu, administrador de sistema da empresa de serviços de TI holandesa Levi9, e afeta todas as versões do firmware do Android 4.x no Galaxy Nexus, Nexus 4 e Nexus 5. Alecu apresentou a vulnerabilidade na sexta-feira (29), durante a conferência de segurança DefCamp em Bucareste, na Romênia.

A SMS classe 0, ou Flash SMS, é um tipo de mensagem definida na especificação GSM que é exibida diretamente na tela do telefone e não fica automaticamente armazenada no dispositivo. Depois de lerem essa mensagem, os usuários têm a opção de salvá-la ou rejeitá-la.

Em smartphones Google Nexus, quando a mensagem é recebida, ela é exibida no topo de todas as janelas ativas e é contornada por uma camada preta semi-transparente, que possui um efeito de escurecimento sobre o restante da tela. Se a primeira mensagem não for guardada ou descartada, e uma segunda mensagem for então recebida, esta última é posicionada por cima da primeira e o efeito de escurecimento aumenta.

Quando tais mensagens são recebidas, não há notificação de áudio, mesmo que esse tipo de aviso esteja configurado para mensagens SMS. Isso significa que os usuários que recebem as mensagens Flash não terão conhecimento sobre elas, até que olhem para o telefone.

Alecu descobriu que, quando um grande número de mensagens Flash - cerca de 30 - é recebido e não é dispensado, os dispositivos Nexus reagem de maneiras inesperadas.

O comportamento mais comum é que o telefone seja reiniciado, disse o pesquisador. Neste caso, se um PIN for necessário para desbloquear o cartão SIM, o telefone não irá se conectar à Internet após a reinicialização e o usuário pode não perceber o problema por horas, até que olhe para o telefone. Durante esse tempo, o celular não será capaz de receber chamadas, mensagens ou outros tipos de notificações que necessitam de uma conexão de rede móvel.

Exceções

De acordo com Alecu, um comportamento diferente que acontece em raras ocasiões é o smartphone não reiniciar, mas temporariamente perder a conexão com a rede móvel. A conexão é automaticamente restaurada e o telefone pode receber e fazer chamadas, mas já não pode acessar a Internet por meio da rede móvel. O único método para restaurar a conexão de dados é reiniciar o telefone, disse Alecu.

Em outras situações raras, apenas o aplicativo de mensagens não funciona, mas o sistema é reiniciado automaticamente e, portanto, não há impacto a longo prazo.

Durante a conferência, o pesquisador realizou um teste ao vivo em um telefone Nexus 4 com a tela desbloqueada e rodando o Android 4.3 - e não resultou em uma reinicialização. No entanto, depois de receber cerca de 30 mensagens classe 0, o telefone travou: toques ou tentativas de bloqueio de tela não funcionavam. Enquanto neste estado, o telefone não pôde receber chamadas e teve que ser reiniciado manualmente.

Uma segunda tentativa com a tela bloqueada também não conseguiu reiniciar o smartphone, porque apenas duas das mais de 20 mensagens foram imediatamente recebidas. Isso pode ter sido causado por um problema de rede ou o operador impôs um limite de recebimento. As

A utilização deste artigo é exclusiva para fins educacionais.

mensagens acabaram por chegar mais tarde e o telefone reiniciou quando a tela foi desbloqueada.

Alecu disse ter descoberto o problema há mais de um ano e, desde então, testou e confirmou a questão em dispositivos Galaxy Nexus, Nexus 4 e Nexus 5 que rodam diversas versões 4.x do Android, incluindo o recém-lançado Android 4.4, ou KitKat.

Cerca de 20 diferentes dispositivos de vários fabricantes também foram testados e não são vulneráveis a esse problema, disse ele. Mas isso não exclui a possibilidade de que alguns dispositivos de outros fornecedores sejam vulneráveis - mas até o momento a questão foi confirmada somente nos celulares Nexus mencionados.

Alecu afirma ter contatado o Google várias vezes desde que descobriu a falha, mas a maioria das respostas que obteve foram automáticas. Alguém da Equipe de Segurança do Android respondeu em julho e disse que a questão seria corrigida no Android 4.3, mas não o foi, de acordo com o pesquisador - o que, segundo ele, contribuiu para sua decisão de divulgar o problema publicamente.

"Agradecemos a ele nos alertar sobre o possível problema e estamos investigando", disse um representante do Google por e-mail.

Fonte: IDGNOW [Portal]. Disponível em: <http://idgnow.uol.com.br/mobilidade/2013/12/02/smartphones-google-nexus-sao-vulneraveis-a-ataques-ddos-via-sms/>. Acesso em: 3 dez. 2013.

A utilização deste artigo é exclusiva para fins educacionais.