Agosto de 2014

Estudo Trimestral IBM X-Force de Inteligência contra Ameaças

Veja o Heartbleed mais de perto – desde a atividade de ataque mais recente até as estratégias de investigação – usando os dados do primeiro semestre de 2014 e pesquisas em andamento

IBM

Índice

Visão geral executiva

Bem-vindo ao estudo trimestral mais recente da equipe de pesquisa e desenvolvimento da IBM X-Force. Neste estudo, veremos como a vulnerabilidade do Heartbleed – CVE-2014-0160, divulgada em abril de 2014 – impactou as organizações no mundo todo. Nosso foco será analisar como os invasores continuam a tirar vantagem desta vulnerabilidade disseminada, revisar as potenciais estratégias de investigação e avaliar como a divulgação é comparada ao restante de nossos dados do primeiro semestre de 2014.

Até agora, a revelação da vulnerabilidade de Heartbleed na biblioteca de OpenSSL foi o maior evento a atingir a indústria de segurança em 2014. O erro permitiu acesso não autenticado tanto a partir de servidores quanto de clientes. Enquanto o impacto inicial de Heartbleed diminui, uma segunda onda de novas vulnerabilidades, encontradas dentro do software livre e reutilizável, merece mais discussão.

Os servidores do mundo todo continuam a ser afetados por esta séria vulnerabilidade, por isso gostaríamos de investigar o que aconteceu desde que a divulgação de Heartbleed pegou tantas organizações de surpresa. A falha fez com que não apenas os pesquisadores focassem na procura de novas áreas de vulnerabilidades dentro do código reutilizável e de softwares livres, como deram aos invasores uma outra ótima oportunidade de usar os métodos de ataque de um dia.

Com a ajuda dos IBM Managed Security Services (MSS), veremos, primeiro, como as organizações lidaram com a consequência imediata do anúncio de Heartbleed, enquanto também adotaram as estratégias de investigação prática e de larga escala para proteção contínua. Em seguida, de uma perspectiva de ataque, nossos pesquisadores do X-Force explicarão o que os invasores podem estar procurando e tentando alcançar com este tipo de vulnerabilidade.

Neste relatório, você aprenderá como uma vulnerabilidade inesperada, generalizada e difícil de corrigir, como o Heartbleed, força as organizações a irem mais longe em seus processos de gerenciamento de risco e comunicação crítica. Em especial, isso se aplica aos principais fornecedores de software que integraram o OpenSSL a suas ofertas e produtos comerciais. Além de se protegerem contra ataques iminentes a seus próprios sistemas potencialmente vulneráveis, os fornecedores também executaram uma análise completa em seus produtos – ou seja, eles tiveram que determinar se algum produto estava usando esta biblioteca de software livre para fornecer correções.

Por razões como essas, o Heartbleed teve um impacto de risco muito maior do que qualquer outros tipos de vulnerabilidades; entretanto, as consequências não foram tão desastrosas como poderiam ter sido. Somente algumas violações atribuídas ao Heartbleed, apesar de ter sido uma vulnerabilidade na tecnologia de núcleo que protege o e-commerce e ajuda a assegurar a privacidade.

Finalmente, concluiremos o relatório com uma visão de como o Heartbleed se compara a outras vulnerabilidades publicamente divulgadas e como este ponto intermediário de 2014 pode ser comparado aos anos anteriores. A boa notícia é que a tendência de divulgação geral está diminuindo. No entanto, ao comparar o impacto real do Heartbleed à sua avaliação de Common Vulnerability Scoring System (CVSS) – que é somente um risco 5.0 ou "médio" – nossos pesquisadores observaram uma importante disparidade. Discutiremos algumas deficiências no padrão de CVSS atual, as inconsistências na pontuação através de organizações diferentes e a perda de confiança na pontuação CVSS como uma medida de risco precisa e confiável. Em seguida, explicaremos como a próxima liberação da versão 3 de CVSS é esperada para direcionar muitas preocupações da indústria de segurança.

O que é Heartbleed?

A vulnerabilidade do Heartbleed é um erro no OpenSSL, um protocolo de software livre popular muito usado na internet, que permite a qualquer pessoa, que saiba como explorar a vulnerabilidade, acessar e ler a memória de sistemas, que deveria ser protegida.

As versões vulneráveis do OpenSSL permitem o comprometimento de chaves secretas, nomes de usuários, senhas e até o conteúdo real. Muitos especialistas em segurança acreditam que esta vulnerabilidade já exista há, pelo menos, dois anos e possa estar sendo explorada desde então. Embora muitas empresas tenham emitido declarações alegando que corrigiram a vulnerabilidade em seus ambientes, não há, na verdade, como saber a quantidade de dados que foram parar em mãos erradas durante a exploração dessa vulnerabilidade.

Para mais informações sobre o Heartbleed, consulte o post do blog do IBM Security Intelligence de abril de 2014[1] ou o website do Heartbleed.[2]

Atividade de ataque de Heartbleed: Antes e agora

Qual foi o impacto real do Heartbleed? Saiba como as ondas de ataques afetaram os clientes dos IBM Managed Security Services.

No dia 7 de abril de 2014, ocorreu um dos eventos de segurança mais importantes dos últimos anos – quando a vulnerabilidade do Heartbleed em OpenSSL (CVE-2014-0160) foi publicamente divulgada. O erro foi introduzido há aproximadamente dois anos e deixou mais de meio milhão de servidores vulnerável para vazamentos de dados não criptografados da memória de sistema com um rastreio mínimo de exploração. A divulgação causou pânico em uma ampla gama de indústrias, agências governamentais e grupos de consumidores que haviam usado o OpenSSL para manter suas transações privadas – encontrando-se, assim, vulneráveis a um ataque e sem qualquer prova de quando os vazamentos ocorreram (ou seja, sem evidência de arquivo de log).

Quase ao mesmo tempo em que a vulnerabilidade foi liberada como uma recomendação de OpenSSL, os IBM Managed Security Services (MSS) testemunharam invasores adquirindo novas ferramentas e explorando o erro imediatamente, em escala mundial. Uma vez que os principais fornecedores de sistemas de detecção de invasão e de prevenção criaram assinaturas de proteção, os MSS puderam ver quão ruim a situação tinha se tornado. No dia 15 de abril 2014, os MSS testemunharam o maior pico na atividade através da base de cliente, com mais de 300.000 ataques em um único período de 24 horas. Isso é uma média de 3,47 ataques por segundo para mais de centenas de clientes.

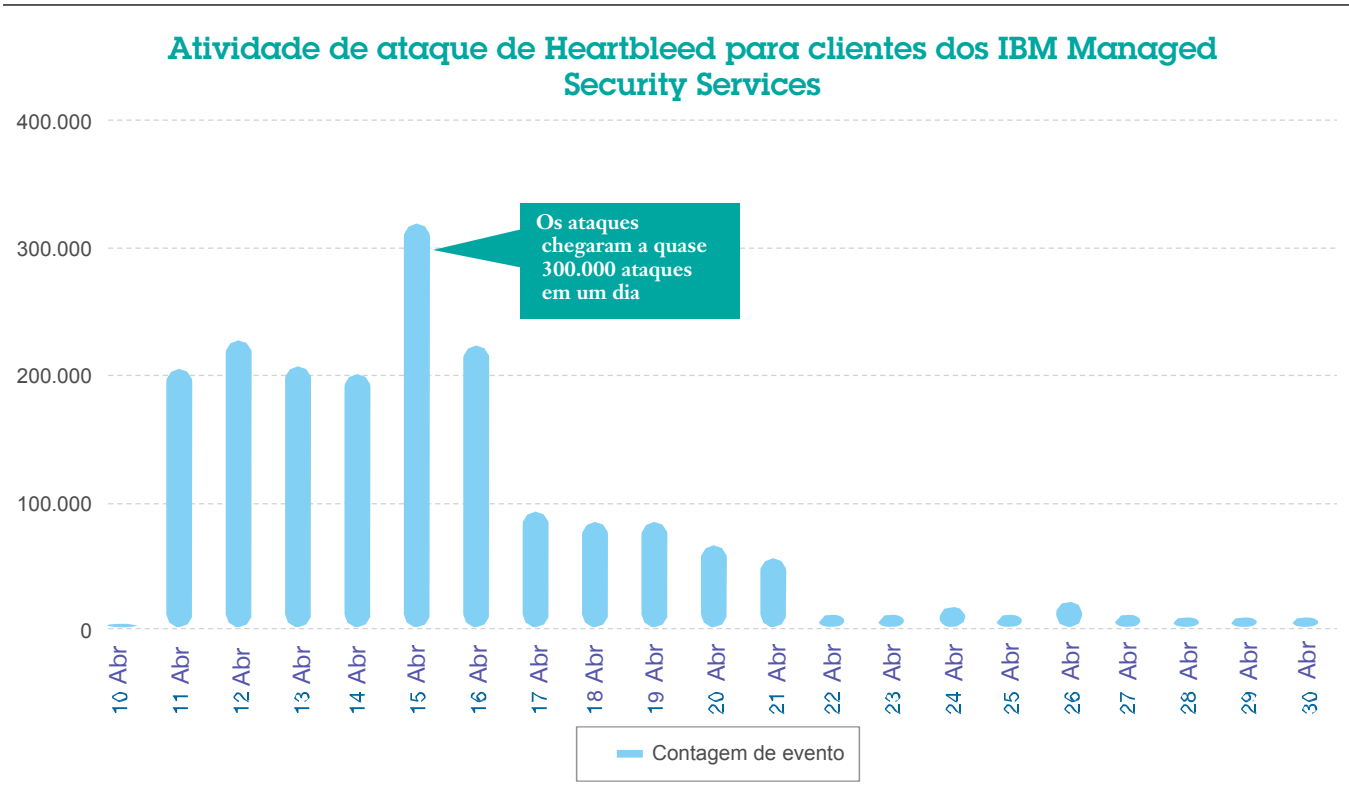

Figura 1. A atividade de ataque foi relacionada à vulnerabilidade do Heartbleed, como observado para clientes dos IBM Managed Security Services, em abril de 2014

Execução da atividade de ataque

Vejamos mais de perto a atividade de ataque após a divulgação do Heartbleed. Ao invés de um único endereço de IP executar repetidamente o ataque, muitos dos ataques usaram um método distribuído. Uma ampla faixa de endereços IP, através de vários números de sistema autônomos (ASNs), atacou as redes monitoradas pelos MSS. Aliás, faixas inteiras de endereços IP atacaram vários servidores de uma vez. Isso permitiu que os invasores tivessem uma superfície de ataque ampla e diversificada e a flexibilidade de superar as estratégias de bloqueio rudimentares.

O que são números de sistema autônomos?

Na Internet, um sistema autônomo refere-se a um grupo conectado de um ou mais prefixos de roteamento de Protocolo de Internet, executado por um ou mais operadores, a fim de suportar uma política de roteamento única e claramente definida. Cada sistema autônomo é designado a um número de roteamento exclusivo global, conhecido como um número de sistema autônomo (ASN).

Originalmente, os sistemas autônomos eram controlados em nome de uma única entidade, como um provedor de serviços à Internet (ISP) ou uma organização muito grande com conexões independentes a múltiplas redes. Agora, várias organizações podem executar o Protocolo de Roteamento de Borda (BGP) usando ASNs privados que ficam atrás de um ISP. Embora vários sistemas autônomos possam ser suportados pelo ISP, a internet vê somente a política de roteamento do ISP, Portanto, somente o ISP deve ter um ASN oficialmente registrado.

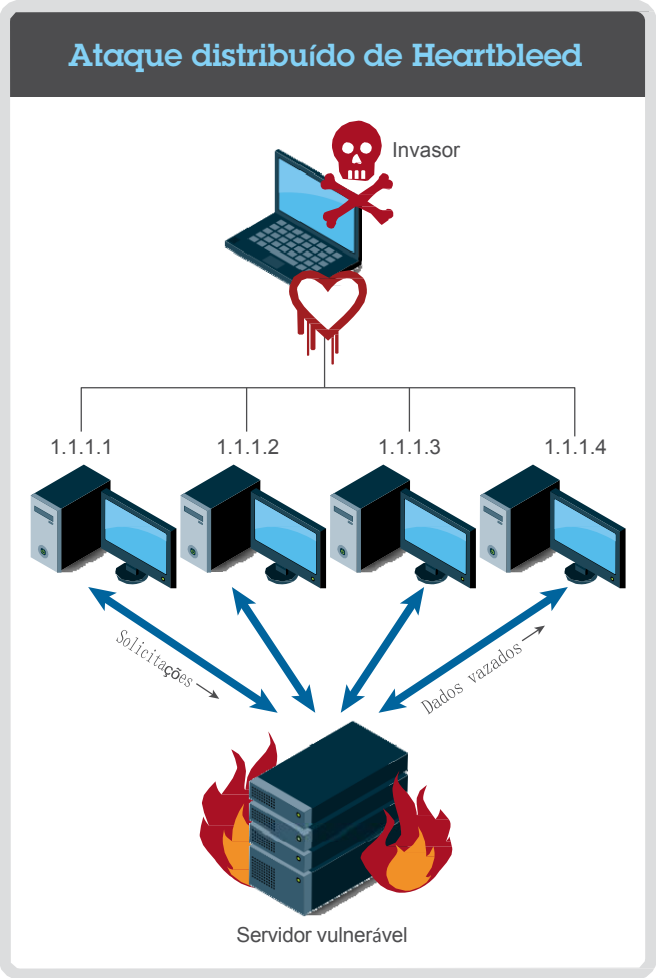

Gráfico 1. Ataque distribuído de Heartbleed

Os ataques diminuíram depois do dia 22 de abril de 2014. Entretanto, a Figura 2 mostra que, apesar da nivelação da atividade de ataque, o número de clientes invadidos permaneceu relativamente consistente ao longo do tempo. Por quê? Como as grandes organizações vulneráveis ao Heartbleed podiam aplicar a correção enviada para a sua infraestrutura, renderizaram os ataques mais infrutíferos. Como resultado, os invasores invasores mudaram o foco para outras explorações. Os MSS testemunharam uma queda importante nos números de IPs de origem gerando ataques e o número total de ataques globais contra a base de clientes dos MSS.

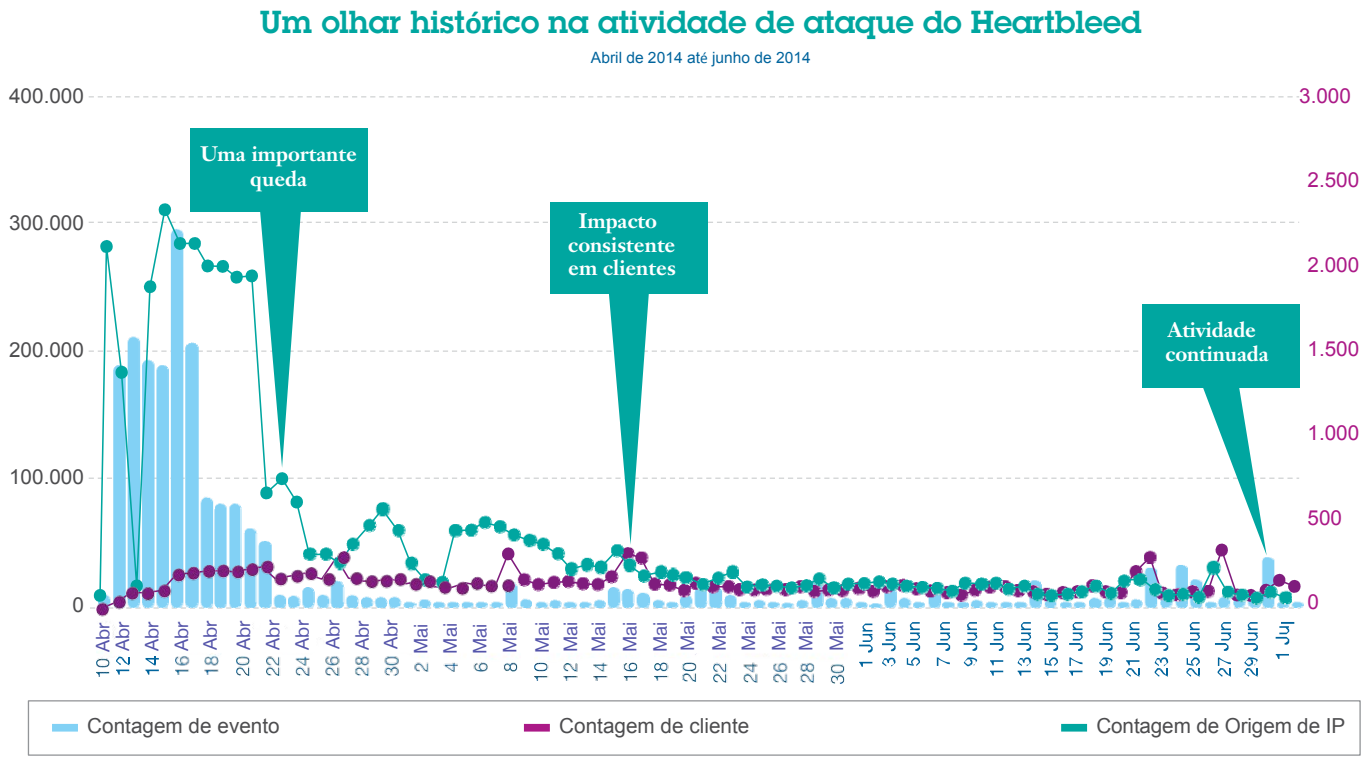

Figura 2. Um olhar histórico na atividade de ataque do Heartbleed a clientes dos IBM Managed Security Services, de abril de 2014 a junho de 2014

No entanto, o estado atual de ataques ainda é importante. Os MSS veem uma média de 7.000 ataques por dia através de uma grande superfície de ataque. As organizações que aplicaram a correção do OpenSSL em sua infraestrutura nos mecanismos de bloqueio implementados, como sistemas de prevenção de invasão e detecção de invasão, podem respirar tranquilas. De acordo com os relatórios recentes dos MSS, vimos que, apesar da pressa inicial para corrigir os sistemas, aproximadamente 50% dos servidores potencialmente vulneráveis não foram corrigidos – tornando o Heartbleed uma ameça crítica e contínua.

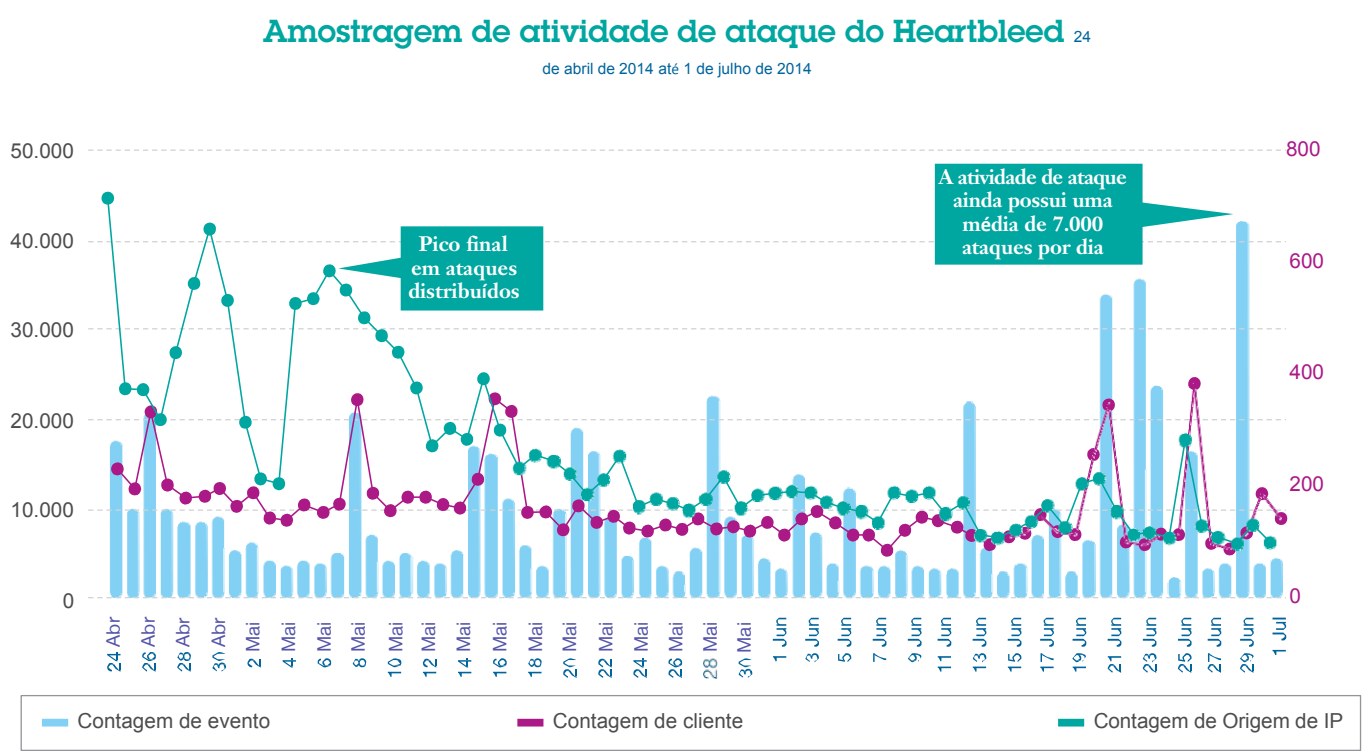

Figura 3. Amostragem de atividade de ataque do Heartbleed a clientes dos IBM Managed Security Services, do dia 24 de abril de 2014 até dia 1 de julho de 2014

Lições aprendidas e recomendações

Foram muitas as lições aprendidas a partir dos dos ataques de Heartbleed. Por exemplo, os MSS descobriram que ter um plano de resposta a incidentes – além de manter um banco de dados de ativo – era absolutamente imprescindível para reduzir a exposição aos ataques. As organizações que tinham lutado para manter um banco de dados de ativo atual ficaram invisíveis para os sistemas que eram vulneráveis e críticos. Ainda que tivessem um plano de resposta a incidentes, era necessário um banco de dados de ativo atualizado para implementá-lo.

Por outro lado, as empresas que tiveram que manter seu banco de dados de ativo e plano de resposta a incidentes puderam implementar rapidamente as correções nos sistemas críticos vulneráveis à ataque, reduzindo, assim, a sua exposição ao Heartbleed. Elas também enfrentaram uma redução importante de riscos para ameaças futuras.

Também é importante compreender as estratégias de detecção e defesa contra ataques, como o Heartbleed. Em certos cenários, as organizações podem utilizar os firewalls para bloquear a massa dos ataques em direção às suas redes. O centro de operações de segurança (SOC) dos MSS aplica essa metodologia quando grandes ataques globais acontecem e a maioria dos ataques tem origem em um pequeno subconjunto de hosts. Esta técnica de bloqueio pode fornecer um adiamento curto e temporário da atividade de ataque, fornecendo um tempo valioso para que os sistemas críticos sejam corrigidos.

Os firewalls são uma defesa excelente quando um pequeno subconjunto de hosts gera os ataques. Além disso, dispositivos de prevenção e detecção de invasão podem fornecer uma proteção ainda maior ao bloquear os ataques que estão no nível de pacote de invasão. Isso diminui a necessidade de manter uma lista ativa de invasores e reduz o risco envolvido, enquanto os sistemas são corrigidos.

A corrida para prevenir ataques de um dia

Descubra quão rápido os invasores correm para explorar a vulnerabilidade, como o Heartbleed – e como é possível investigar a ameaça.

"Quão rápido podemos obter uma correção implementada?" Esta é a questão que a maioria das organizações pergunta a si mesma quando a recomendação de segurança do Heartbleed (CVE-2014-0160) foi publicada no dia 7 de abril de 2014. Imediatamente após o anúncio, as organizações correram para corrigir os seus sistemas. Enquanto isso, somente um dia após a divulgação, uma ferramenta de prova de conceito[3] capaz de explorar o bug do Heartbleed começou a circular, expondo os sistemas não corrigidos tanto para invasores experientes como para os não experientes. O mais alarmante é o fato de que, também um dia depois da revelação, os ataques que alavancaram a vulnerabilidade começaram a ocorrer[4] e as ações de algumas das organizações afetadas na investigação de ataques ou na correção da vulnerabilidade já eram tardias.[5, 6]

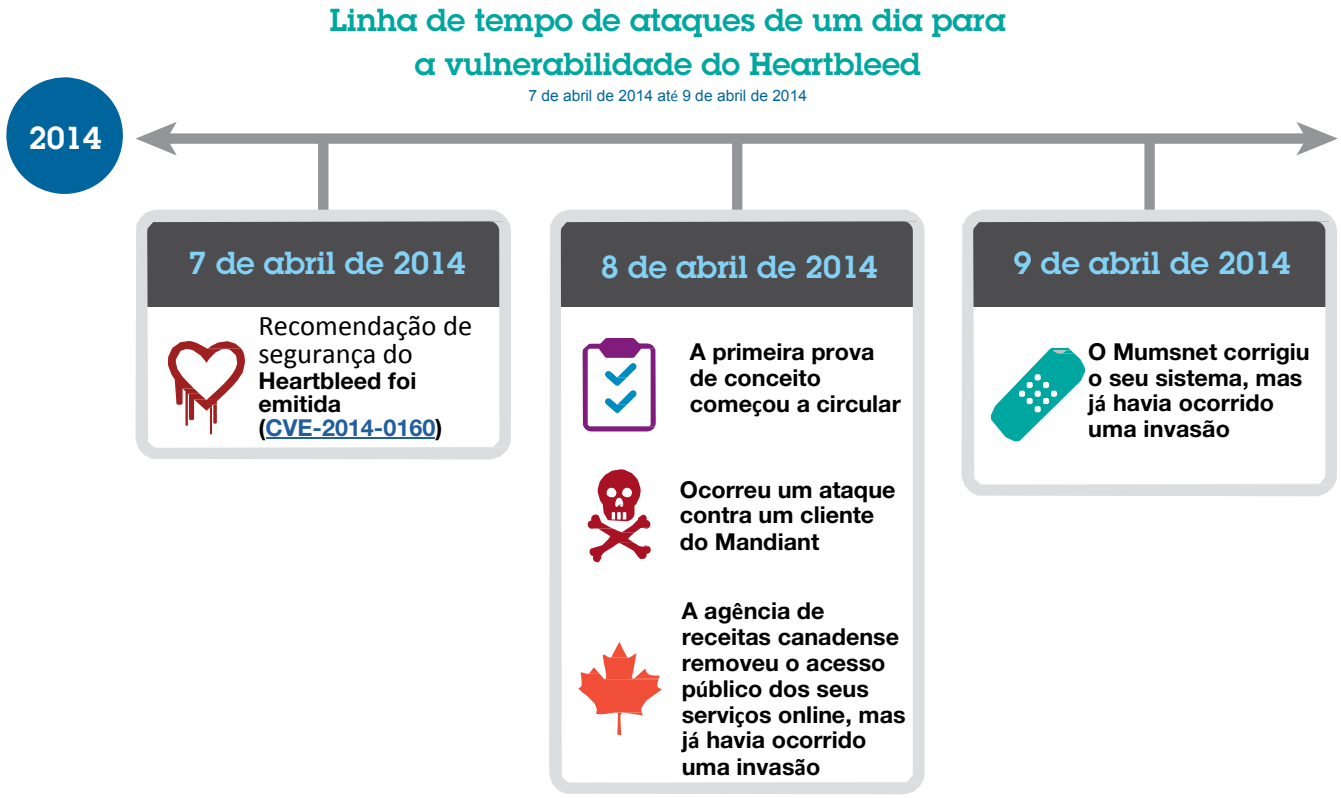

Figura 4. Linha de tempo de ataques de um dia para vulnerabilidade do Heartbleed (CVE-2014-0160), 7 de abril de 2014 até 9 de abril de 2014

As reflexões de ataques de Java em 2012

Não é a primeira vez que os ataques de um dia ocorreram no Heartbleed – ou seja, os ataques alavancam uma vulnerabilidade que já foi corrigida. Na verdade, os analistas do X-Force notaram esta tendência após a divulgação da vulnerabilidade de Java de 2012 (CVE-2012-1723), como discutido em nosso Relatório de Risco e Tendência do IBM X-Force 2012.

No caso dessa vulnerabilidade de Java, um pesquisador de segurança alegou que ele poderia criar uma exploração de prova de conceito somente um dia após uma correção ser emitida para a vulnerabilidade e, uma semana depois, publicou os detalhes da vulnerabilidade.[7] Felizmente, nesse caso em particular, o código de prova de conceito não foi liberado. Entretanto, a integração do código de exploração de trabalho em um kit de exploração em massa[8] – postado somente um mês após a correção tornar-se disponível para a vulnerabilidade – significou que muitos sistemas que ainda não haviam sido corrigidos tornaram-se alvos em potencial por meio de ataques guiados. Posteriormente, a exploração para a vulnerabilidade foi integrada em outros kits de exploração, aumentando, assim, o risco de sistemas não corrigidos serem comprometidos.

Figura 5. Linha de tempo de ataques de um dia para a vulnerabilidade de Java de 2012 (CVE-2012-1723), 12 de junho de 2012 até 11 de julho de 2012

Uma corrida para corrigir

Os exemplos de vulnerabilidade do Heartbleed e do Java demostram que os ataques de um dia podem ser tão perigosos quanto os ataques de dia zero. Diferente dos ataques de dia zero - em que a vulnerabilidade é desconhecida e uma correção não está disponível – o problema com os ataques de um dia está em quanto tempo uma correção leva para ser implementada. O gerenciamento de correção é um desafio complexo, especialmente para implementações grandes e para os sistemas essenciais que exigem um amplo teste de pré-implementação.

Além disso, se a vulnerabilidade estiver em uma biblioteca muito usada, como a biblioteca do OpenSSL como no caso de Heartbleed, o problema será mais complicado, pois as organizações dependem do tempo adicional que os fornecedores de software levam para integrar e testar as correções em seus próprios produtos antes que o produto seja entregue a eles. Este tempo adicional de espera significa uma janela de exposição ampliada da qual os invasores podem tirar vantagem.

Uma corrida para explorar

Do ponto de vista do invasor, as vulnerabilidades recém-corrigidas representam uma oportunidade, já que são pontos potencialmente fracos (embora temporários) em sua infraestrutura alvo. Para os ataques de um dia, o objetivo do invasor é tirar vantagem da janela de exposição das organizações entre o anúncio das correções e a implementação real das correções.

As seções a seguir explicam como os invasores criam as explorações de um dia, para que seja possível entender o quão rápido o ataque armado pode tirar vantagem de uma vulnerabilidade corrigida.

Localizando o erro corrigido

Geralmente, os invasores precisam, em primeiro lugar, identificar o código que foi corrigido em resposta à vulnerabilidade. Para os projetos de software livre, esta é uma tarefa avançada, pois eles podem simplesmente revisar repositórios de código-fonte publicamente acessíveis e check-ins de código-fonte em relação à vulnerabilidade. Para os aplicativos de código fechado, é possível usar um processo chamado “diff binário” para encontrar quais partes do código binário foram alterados, restringindo para as funções alteradas e, por fim, o código vulnerável. Para os invasores experientes, o diff binário pode ser tão simples quanto encontrar as diferenças no código-fonte.

Nossa pesquisa mostrou que um invasor experiente pode encontrar o código vulnerável em somente alguns minutos (no caso de aplicativos de código aberto com os check-ins comentados) ou até em, no máximo, algumas horas (no caso de aplicativos binários com várias alterações não relacionadas).

Explorando o erro

O fator mais importante que influencia quando um invasor pode explorar uma vulnerabilidade é a dificuldade envolvida ao se desenvolver uma exploração ou *armá-la.* Por um lado, há vulnerabilidades que só podem ser exploradas caso o aplicativo esteja em um estado particular e/ou a investigação de exploração seja ignorada. Para esses casos, é necessário mais tempo de pesquisa para desenvolver uma exploração que funcione. Porém, por outro lado, há vulnerabilidades que podem ser exploradas facilmente e as investigações de exploração associadas podem ser ignoradas usando as técnicas previamente usadas ou publicadas.

Um invasor experiente pode desenvolver, em poucas horas, um código de exploração para vulnerabilidades fáceis de serem exploradas. Enquanto que um código de exploração para vulnerabilidades difíceis de serem exploradas pode demorar dias, semanas ou até meses para se desenvolvido, dependendo do nível de dificuldade.

Infelizmente, no caso do Heartbleed, o desenvolvimento do código de exploração era avançado, como evidenciado pela liberação do código de exploração somente um dia após a divulgação.

Investigações

A corrida para implementar as correções e desenvolver as explorações não será sempre vencida pelas organizações e é prudente assumir que, na maioria dos casos, os invasores podem vencer. Entretanto, existem maneiras de as organizações melhorarem a sua postura em relação aos ataques de um dia enquanto as correções estão sendo testadas e implementadas:

- **Aplicar soluções alternativas.** Verifique se o fornecedor disponibilizou orientação para uma solução alternativa temporária que possa ajudar a evitar a exploração da vulnerabilidade. Isso pode envolver a mudança de uma configuração específica ou a desativação temporária de um módulo ou um recurso em que a vulnerabilidade exista ou seja usada como um vetor para a exploração da vulnerabilidade.

- **Bloquear os ataques.** Os produtos de segurança – como sistemas de detecção de invasão ou prevenção de invasão e software de antivírus – podem servir como uma primeira linha de defesa contra a exploração de vulnerabilidades enquanto as correções estão sendo testadas e implementadas. Os programas de fornecedores, como o Microsoft Active Protections Program (MAPP)[9], disponibilizam, às empresas de software de segurança, o primeiro acesso a informações de vulnerabilidade, de modo que, quando as correções da Microsoft são liberadas, os fornecedores de segurança possam liberar imediatamente o conteúdo de segurança que pode ajudar a detectar e bloquear as explorações contra as vulnerabilidades recentemente corrigidas.

- **Encerrar temporariamente os sistemas.** Embora os líderes de negócio possam ser contra, outra solução é encerrar temporariamente ou desconectar o sistema afetado enquanto uma correção estiver sendo testada. Esta opção pode ser a melhor maneira de ajudar a evitar a perda de informações pessoais ou financeiras dos clientes. Se o encerramento temporário de um sistema vulnerável ajudar a parar o roubo de informações, provavelmente os clientes irão entender o porquê de um serviço estar temporariamente indisponível.

Os invasores são oportunistas. Eles agarrarão qualquer oportunidade para atacar quando o alvo estiver em um estado mais fraco. Para uma organização, a melhor defesa contra ataques de um dia é estar pronta – ter planos de ação preparados e investigações posicionadas quando uma vulnerabilidade crítica for relatada.

Divulgações de vulnerabilidades no primeiro semestre de 2014

Qual é o estado de segurança depois do Heartbleed? Conhe- a as tendências de divulgação deste ano e as alterações para a avaliação da vulnerabilidade.

Desde 1997, o X-Force vem rastreando as divulgações de vulnerabilidades nos produtos de software, como a divulgação do Heartbleed (CVE-2014-0160) no começo do do ano. Nossos pesquisadores do X-Force coletaram as recomendações de software dos fornecedores e as listas de correio relacionadas à segurança, e analisaram centenas de vulnerabilidades de páginas da web em que os dados de correção, as explorações e as vulnerabilidades foram divulgadas.

No primeiro semestre de 2014, relatamos mais de 3.900 novas vulnerabilidades de segurança afetando 926 fornecedores exclusivos. Se essa tendência continuar até o final do ano, o total previsto de vulnerabilidades cairia abaixo de 8.000 vulnerabilidades totais pela primeira vez desde 2011.

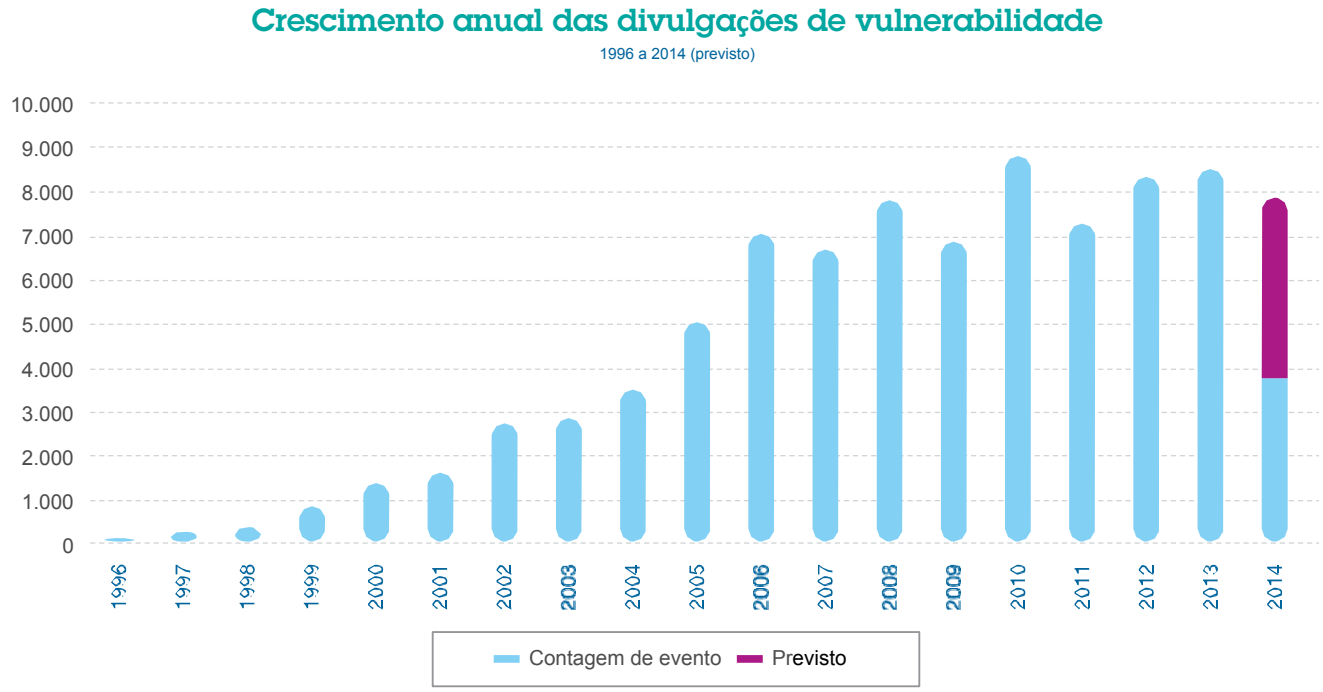

Figura 6. Crescimento anual das divulgações de vulnerabilidade, de 1996 até 2014 (previsto)

É difícil apontar para qualquer fator que tenha contribuído com o declínio no número de divulgações de vulnerabilidade em 2014. Entretanto, é interessante observar que o número total de fornecedores divulgando vulnerabilidades diminuiu ano após ano (1.602 fornecedores em 2013, em comparação a 926 fornecedores em 2014).

Mesmo com o declínio previsto no número total de divulgações de vulnerabilidade em 2014, o número de vulnerabilidade divulgado pelos maiores fornecedores de software corporativo permaneceu praticamente o mesmo, ano após ano (34% em 2013, em comparação a 32% em 2014), como mostrado na Figura 7.

Ao analisar tendências em softwares corporativos, a equipe do X-Force leva em consideração os fornecedores de software que criaram a maior variedade de softwares corporativos. Foi observado que, dentre milhares de fornecedores, essas empresas divulgaram de maneira consistente um número importante de vulnerabilidades de segurança. Nós categorizamos esses fornecedores em um grupo dos 10 melhores, ignorando as vulnerabilidades de sistema de gerenciamento de conteúdo (CMS), já que a maioria delas está nos plug-ins e complementos de terceiros e não é tão usada como software de nível empresarial. Geralmente, esses fornecedores possuem uma abordagem mais ampla de segurança, que inclui políticas e práticas para direcionar e responder às vulnerabilidades de segurança, o que leva a um número maior de divulgações públicas de vulnerabilidade.[10]

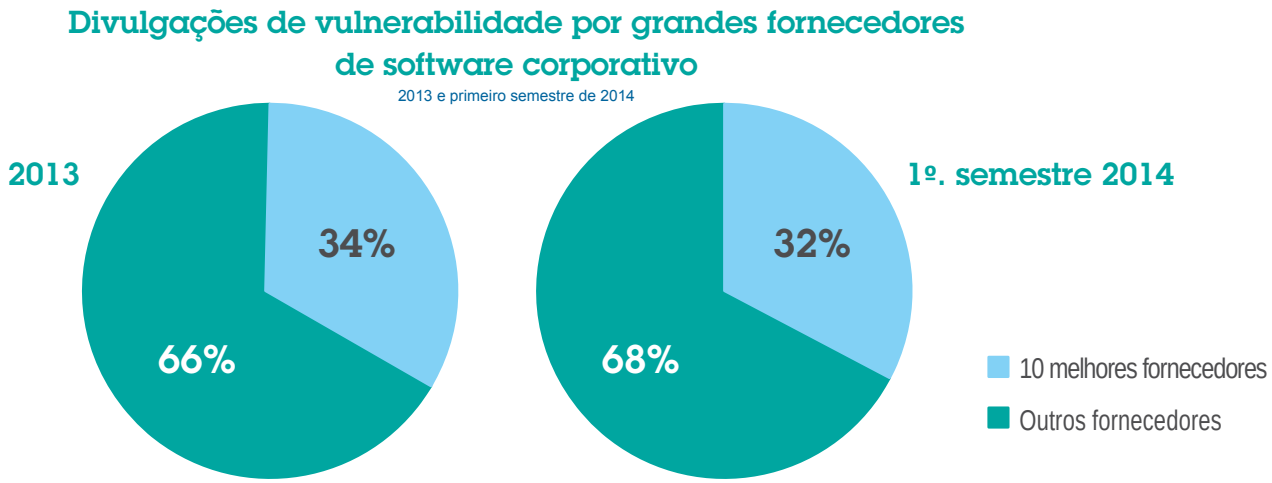

Figura 7. Divulgações de vulnerabilidade por grandes fornecedores de software corporativo, 2013 e primeiro semestre de 2014

Vulnerabilidades em sistemas de gerenciamento de conteúdo

Vulnerabilidades em CMS continuam a estar entre as mais relatadas em 2014, contabilizando quase 10% do total de vulnerabilidades totais pesquisadas. E, além disso, a maior porcentagem de vulnerabilidades de CMS ocorre em plug-ins ou módulos escritos por fontes de terceiros – não pelo fornecedor principal de CMS.

Muitos plug-ins de CMS são mantidos por uma pessoa ou um pequeno grupo e eles podem ter atualizações não frequentes (ou nenhuma). Portanto, muitos plug-ins contêm vulnerabilidades de segurança tentadoras e não corrigidas. A Figura 8 mostra o atraso nas taxas de correção para plug-ins, em comparação às plataformas principais de CMS, e os dados não se alteraram desde nosso relatório de 2013.

Enquanto o X-Force alertava previamente para o uso de plug-ins de CMS, uma nova onda de ataques contra essas plataformas foi lançada nos últimos meses, mostrando o risco continuado. O site russo Yandex relatou um malware com dub efetuado no Vírus Mayhem[11] que visa comprometer os servidores da web por meio das vulnerabilidades de CMS e ataques de força bruta de credenciais fracas ou padrão.

Depois de comprometidos, esses servidores da web podem ser usados como malwares ou carregar ataques de grandes escala e largura de banda de distributed-denial-of-service (DDoS) contra outros sites e alvos. Por exemplo, o WordPress foi usado em um ataque de DDoS de amplificação em março de 2014, que afetou mais de 162.000 sites.[12] Nesse caso, os invasores usaram a funcionalidade legítima do recurso de pingback de XML-RPC para conectar o conteúdo de autores diferentes a um website de terceiros.

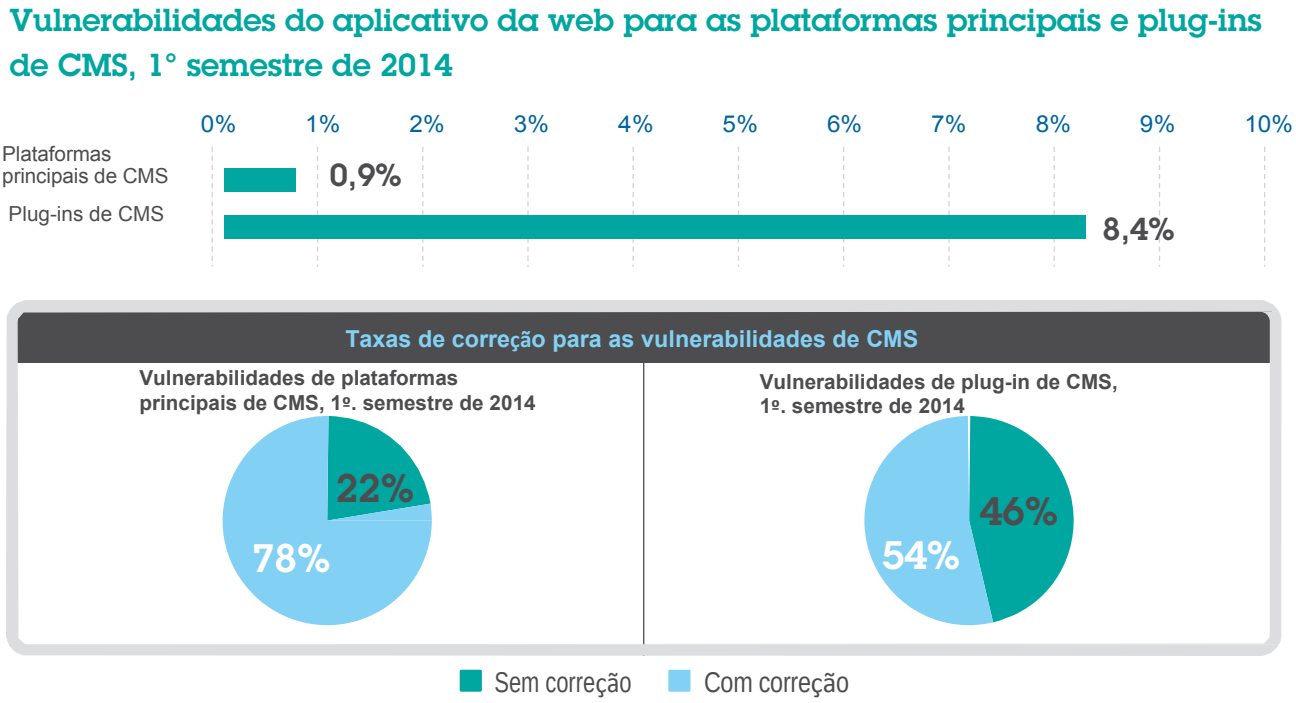

Figura 8. Vulnerabilidades do aplicativo da web para plataformas principais de CMS e plug-ins de CMS, como uma porcentagem de todas as taxas de divulgações e correções correspondentes, 1º.semestre de 2014.

Avaliação de CVSS

O X-Force usa a versão 2 do Common Vulnerability Scoring System (CVSS) para comunicar a severidade das vulnerabilidades. As vulnerabilidades são avaliadas a partir de três perspectivas diferentes: como um banco de dados de vulnerabilidade que rastreia as divulgações de vulnerabilidades de terceiros; como uma organização de pesquisa de segurança que descobre novas vulnerabilidades; e como um grande fornecedor de software que necessita ajudar os clientes a avaliar com precisão a severidade de vulnerabilidades em seus produtos. O X-Force está trabalhando atualmente junto com outras organizações no desenvolvimento do novo CVSS, versão 3.[13]

Na avaliação de vulnerabilidades do primeiro semestre de 2014, foi descoberto que a maioria dos problemas se encaixava na categoria de taxa de severidade média de CVSS (67%), com 24% de todas as vulnerabilidades avaliadas como críticas ou altas. Como mostrado na Figura 9, esses resultados não foram alterados desde 2013, sendo este o terceiro ano consecutivo em que a maioria das vulnerabilidades foi avaliada como riscos de nível médio.

Avaliações de base de CVSS de 2012 até o 1º, semestre de 2014

Avaliação	Nível
10	**Crítico** É provável que uma exploração bem-sucedida tenha efeitos adversos catastróficos
7.0 – 9.9	**Alto** É provável que uma exploração bem-sucedida tenha efeitos adversos importantes
4.0 – 6.9	**Médio** É provável que uma exploração bem-sucedida tenha efeitos adversos moderados
0.0 – 3.9	**Baixo** É provável que uma exploração bem-sucedida tenha efeitos adversos limitados

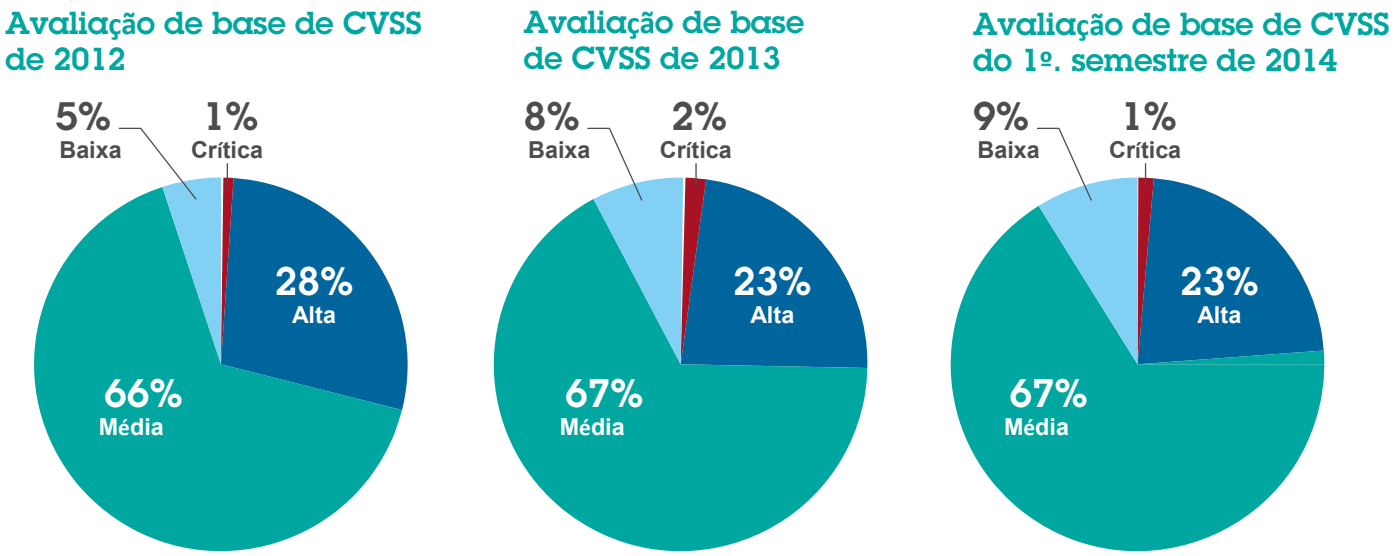

Figura 9. Avaliações de base de CVSS de 2012 até o 1º.semestre de 2014

Muitas pessoas da indústria, inclusive analistas de segurança, equipes de resposta de incidentes corporativos e clientes de software corporativo, ficaram insatisfeitas com as inconsistências de avaliação que ocorrem com frequência em diferentes organizações. Às vezes, as inconsistências são o resultado da subjetividade que pode influenciar em como um indivíduo ou organização avalia as vulnerabilidades, mas também podem resultar de algumas falhas inerentes no padrão atual de CVSS e da falta de orientações claras em como avaliar objetivamente certos tipos de vulnerabilidades. Como resultado, a contagem de CVSS falha com frequência em refletir o verdadeiro risco que uma vulnerabilidade pode representar para uma organização, causando uma perda de confiança geral na avaliação de CVSS como uma medição de risco precisa e confiável.

Para saber mais sobre os interesses acerca de CVSS e o desenvolvimento do novo CVSS, versão 3, consulte o website do CVSS v3 Development, hospedado pelo Forum of Incident Response and Security Teams (FIRST).[13]

O exemplo mais óbvio de como algumas avaliações de CVSS nem sempre representam os verdadeiros riscos e impactos em uma organização é a vulnerabilidade de Heartbleed. Como mencionado anteriormente neste relatório, o Heartbleed foi divulgado em abril de 2014, mas, na verdade, já existia há dois anos. Essa vulnerabilidade recebeu uma avaliação de base de CVSS de 5.0, que se encaixa no nível de risco médio – junto com 67% de todas as outras vulnerabilidades relatadas durante o primeiro semestre de 2014.

Entretanto, com o número de produtos impactados, o tempo e a atenção gastos pelas equipes de TI para corrigir os sistemas e responder às questões do cliente, assim como a sensibilidade dos dados expostos, o verdadeiro impacto da vulnerabilidade de Heartbleed foi maior que a avaliação de base de CVSS poderia indicar. Isso também levanta a questão de quais outras vulnerabilidades se encaixam na categoria de risco médio (avaliação de base de CVSS 4.0 até 6.9), que podem ter sido ignoradas pelas organizações, mas que também tinham impactos potenciais de grande escala similar ao Heartbleed.

Considerações finais sobre primeiro semestre de 2014

Embora os números gerais de vulnerabilidade estejam baixos para o primeiro semestre de 2014, o impacto nos 10 melhores fornecedores de software corporativo permaneceu consistente. Neste ponto, é incerto se essa tendência permanecerá até o final do ano, com os invasores continuando a procurar os alvos com o maior impacto//potencial de recompensa, ou se veremos, no segundo semestre do ano, um aumento no no número de vulnerabilidades divulgadas contra os fornecedores e componentes menores, como os plug-ins de CMS.

O X-Force também antecipa a liberação e adoção da versão 3 do CVSS para ajudar a criar mais consistência na avaliação de risco por parte das organizações e mais confiança no uso de CVSS, como um dos componentes primários em um plano de resposta a incidentes geral da organização. Dessa forma, quando divulgações como o Heartbleed ocorrerem no futuro, a indústria, como um todo, estará mais bem preparada para ameaças em potencial.

Sobre o X-Force

As ameaças avançadas estão em toda parte. Ajude a minimizar os seus riscos com insights dos especialistas da IBM.

A equipe de pesquisas e desenvolvimento da IBM X-Force estuda e monitora as tendências de ameaças mais recentes, inclusive vulnerabilidades, explorações, malware, spam, phishing e conteúdo malicioso da web. A equipe de pesquisa inclui uma variedade de conjuntos de habilidades e conhecimento, impulsionados com as aquisições da IBM no mercado de segurança de Internet – incluindo a Internet Security Systems (ISS), IBM Trusteer[14] e IBM Security AppScan – e combinando-os com inteligência de monitoração ativa da rede do grupo do IBM Managed Security Services. Além de aconselhar os clientes e o público em geral sobre as ameaças críticas e emergentes, o IBM X-Force também oferece conteúdo de segurança e técnicas de proteção para ajudar a proteger os clientes IBM dessas ameaças.

Colaboração da IBM Security

A IBM Security representa várias marcas que oferecem um grande espectro de competência de segurança:

- As equipes de pesquisa e desenvolvimento de vulnerabilidade do IBM X-Force descobrem, analisam, monitoram e registram uma ampla gama de ameaças de segurança a computadores, vulnerabilidades, além de tendências e métodos mais recentes usados pelos invasores. Outros grupos da IBM utilizam esses valiosos dados para desenvolver técnicas de proteção aos nossos clientes.
- A família de produtos IBM Trusteer fornece uma plataforma de prevenção de crimes na web de terminal holístico que ajuda a proteger as organizações contra fraude financeira e invasões de dados. Centenas de organizações e milhões de usuários finais dependem desses produtos da IBM Security para proteger os seus aplicativos de web, computadores e dispositivos móveis de ameaças online (como malwares avançados e ataques de phishing).
- A equipe de segurança de conteúdo da IBM X-Force vasculha e categoriza independentemente a web por crawl, descobertas independentes e por feeds fornecidos pelos IBM Managed Security Services.
- O IBM Managed Security Services é responsável por monitorar as explorações relacionadas a endpoints, servidores (inclusive servidores da web) e infraestrutura de rede geral. Essa equipe rastreia as explorações entregues pela web e também por outros vetores, como emails e mensagens instantâneas.
- O IBM Professional Security Services (PSS) oferece serviços corporativos de consultoria de avaliação, design e implementação de segurança para ajudar a desenvolver soluções efetivas de segurança da informação.
- A Plataforma de Inteligência em Segurança IBM QRadar oferece uma solução integrada para Security Intelligence and Event Management (SIEM), gerenciamento de registros, gerenciamento de configuração, avaliação de vulnerabilidade e detecção de anomalias. Ele fornece um painel unificado e um insight em tempo real sobre os riscos de segurança e conformidade de pessoas, dados, aplicativos e infraestrutura. O IBM Security AppScan permite que as organizações
- avaliem a segurança de aplicativos móveis e da web, fortaleçam o gerenciamento de programas de segurança de aplicativos e obtenham conformidade regulatória pela identificação de vulnerabilidades e geração de relatórios com recomendações inteligentes para facilitar as correções. O serviço de IBM Hosted Application Security Management (HASM) é uma solução baseada em nuvem para testar aplicativos da web com o uso do AppScan em ambientes de pré-produção e produção.

Colaboradores

A produção do Estudo trimestral sobre Inteligência contra ameaças da IBM X-Force é uma colaboração dedicada por toda a IBM. Gostaríamos de agradecer às seguintes pessoas pela atenção e contribuição para a publicação deste relatório.

Colaborador	Cargo
Brad Sherrill	Manager, IBM X-Force Threat Intelligence Database
John Kuhn	Senior Threat Researcher, IBM Managed Security Services
Leslie Horacek	Manager, IBM X-Force Threat Response
Lyndon Sutherland	Threat Intelligence Analyst, IBM Managed Security Services
Mark Yason	Senior Threat Researcher, IBM X-Force Advanced Research
Entalhe Bradley	Practice Lead, Threat Research Group
Pamela Cobb	Worldwide Market Segment Manager, IBM X-Force and IBM Security Threat Portfolio
Robert Freeman	Manager, IBM X-Force Advanced Research
Scott Moore	Software Developer, Team Lead, IBM X-Force Threat Intelligence Database
Thomas Van Tongerloo	Senior Cyber Threat Analyst, IBM Managed Security Services
Troy Bollinger	Threat Intelligence Analyst, IBM Managed Security Services

Para obter mais informações

Para saber mais sobre a IBM X-Force, acesse:
ibm.com/security/xforce/

[1] Chris Poulin, "What to Do to Protect against Heartbleed OpenSSL Vulnerability," *Blog do IBM Security Intelligence*, 10 de abril de 2014. http://securityintelligence.com/heartbleed-openssl-vulnerability-what-to-do-protect/

[2] "The Heartbleed Bug," *codenomicon*, 29 de abril de 2014. http://heartbleed.com

[3] "Untitled," *pastebin*, acessado no dia 25 de julho de 2014. http://pastebin.com/qyXE7myF

[4] Christopher Glyer e Chris DiGiamo, "Attackers Exploit the Heartbleed OpenSSL Vulnerability to Circumvent Multi-factor Authentication on VPNs," *blog Mandiant M-unition*, 18 de abril de 2014. https://www.mandiant.com/blog/attackers-exploit-heartbleed-openssl-vulnerability-circumvent-multifactor-authentication-vpns/

[5] "Statement by the Commissioner of the Canada Revenue Agency on the Heartbleed Bug," *Reuters*, 14 de abril de 2014. http://uk.reuters.com/article/2014/04/14/idUKnMKWbNWG8a+1dc+MKW20140414

[6] "The Heartbleed security breed - and what to do," *Mumsnet*, 16 de abril de 2014. http://www.mumsnet.com/info/the-heartbleed-security-breach-to-do

[7] Michael Schierl, "CVE-2012-1723 – Oracle Java Applet Field Bytecode Verifier Cache Remote Code Execution," acessado no dia 25 de julho de 2014. http://schierlm.users.sourceforge.net/CVE-2012-1723.html

[8] Kafeine, "Inside Blackhole Exploits Kit v1.2.4 - Exploit Kit Control Panel," *Malware don't need Coffee*, 22 de julho de 2012. http://malware.dontneedcoffee.com/2012/07/inside-blackhole-exploits-kit-v124.html

[9] "Microsoft Active Protections Program," *Security TechCenter*, acessado no dia 25 de julho de 2014. http://technet.microsoft.com/en-US/security/dn467918

[10] John Lucassen, "Are Vendors Doing What Is Needed to Mitigate Security Vulnerabilities?" *Blog do IBM Security Intelligence*, 30 de junho de 2014. http://securityintelligence.com/are-vendors-doing-what-is-needed-to-mitigate-security-vulnerabilities/#.U9FWSrG7IUi

[11] Swati Khandelwal, "Mayhem – A New Malware Targets Linux and FreeBSD Web Servers," *The Hacker News*, 24 de julho de 2014. http://thehackernews.com/2014/07/mayhem-new-malware-targets-linux-and_24.html

[12] Ryan Barnett, "More than 162,000 WordPress sites used in DDoS attack," *Trustwave SpiderLabs*, 12 de março de 2014. http://blog.spiderlabs.com/2014/03/wordpress-xml-rpc-pingback-vulnerability-analysis.html

[13] Seth Hanford, "Common Vulnerability Scoring System, V3 Development Update," *FIRST*, junho de 2014. http://www.first.org/cvss/v3/development

[14] A Trusteer, Ltd. foi adquirida pela IBM em setembro de 2013.

Recicle

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo – SP
Brasil

O site da IBM pode ser encontrado em:
Ibm.com

WGL03057-BRPT-00