Política de Denúncia de Vulnerabilidades

Introdução

O UnitedHealth Group leva a sério a proteção dos dados de nossos clientes e membros. Somos gratos pelo trabalho investigativo sobre vulnerabilidades de segurança realizado por pesquisadores de segurança éticos e bem-intencionados. Temos o compromisso de colaborar com a comunidade de segurança da informação para investigar e resolver problemas de segurança em nossos sites, serviços on-line e aplicativos móveis que sejam relatados a nós de acordo com esta Política de Denúncia de Vulnerabilidades. Se você tiver informações relacionadas a possíveis vulnerabilidades de segurança dos produtos ou serviços UnitedHealth Group, UnitedHealthcare ou Optum, queremos ouvir o que você tem a dizer.

Recompensas por Bugs

O UnitedHealth Group não oferece um programa de recompensa por bugs ou outras recompensas por divulgações de segurança. No entanto, agradecemos os esforços dos pesquisadores de segurança que dedicam seu tempo para investigar e nos relatar vulnerabilidades de segurança de acordo com esta política.

Escopo

Este programa não é um meio de enviar reclamações sobre os serviços ou produtos do UnitedHealth Group, UnitedHealthcare, Optum ou de suas subsidiárias (doravante denominadas “UnitedHealth Group”), ou para consultas sobre a disponibilidade de sites da empresa ou serviços on-line. Os seguintes tipos de vulnerabilidades são considerados fora do escopo deste programa:

- Vulnerabilidades volumétricas (por exemplo, Denial of Service ou DDoS);
- Denúncias de vulnerabilidades não exploráveis e violação de “melhores práticas” (por exemplo, falta de cabeçalhos de segurança);
- Fraquezas de configuração do Transport Layer Security (TLS) (por exemplo, suporte para conjuntos de cifras “fracos”);
- Divulgação de impressões digitais/banners em serviços comuns/públicos;
- Scripting entre sites (XSS);

- Compartilhamento interno de IP;
- Falsificação de solicitação entre sites (CSRF);
- Métodos HTTP inexploráveis (por exemplo, OPTIONS ou HEAD);
- Mensagens de erro com dados não sensíveis; e
- Falta de sinalizadores seguros/somente HTTP em cookies que não são de sessão.

O UnitedHealth Group pode atualizar esta política a qualquer momento, inclusive fazendo alterações na lista de vulnerabilidades fora do escopo.

Denunciando uma Vulnerabilidade

Se você identificou um problema que acredita ser uma vulnerabilidade dentro do escopo, envie um e-mail para securityreporting@optum.com. Inclua o seguinte, conforme for aplicável:

- Uma descrição detalhada da vulnerabilidade
- URLs completos associados à vulnerabilidade
- Uma Prova de Conceito (POC, *Proof of Concept*) ou instruções (por exemplo, capturas de tela, vídeo, etc.) sobre como reproduzir a vulnerabilidade ou medidas empregadas para explorar a vulnerabilidade
- Campos de entrada, filtros ou outros objetos de entrada envolvidos
- Sua avaliação de risco ou avaliação de exportabilidade
- Instruções sobre como entrar em contato com você com perguntas subsequentes

A sugestão de soluções será aceita, mas não obrigatória, ao relatar uma vulnerabilidade. A falta de uma explicação detalhada da vulnerabilidade pode resultar em atrasos na nossa resposta e em eventuais ações subsequentes relacionadas à descoberta.

Instruções

Esta política proíbe a realização das seguintes atividades:

- Hacking, testes de penetração ou outras tentativas de obter acesso não autorizado a software ou sistemas do UnitedHealth Group;
- Varredura ou teste ativo de vulnerabilidades;
- Divulgação ou utilização de quaisquer informações ou dados proprietários ou confidenciais do UnitedHealth Group, incluindo dados de clientes; ou
- Afetar negativamente a operação de software ou sistemas do UnitedHealth Group.

Os pesquisadores de segurança não devem violar nenhuma lei, nem acessar, usar, alterar ou comprometer de qualquer forma quaisquer dados do UnitedHealth Group.

Se você tiver alguma dúvida sobre esta política ou as orientações acima, entre em contato com nossa equipe de segurança para obter instruções: securityreporting@optum.com.

O que esperar

Após receber uma denúncia de vulnerabilidade, o UnitedHealth Group ou um de seus representantes poderá enviar uma resposta automática como confirmação. O UnitedHealth Group poderá entrar em contato com o(s) denunciante(s) se informações adicionais forem necessárias para auxiliar na investigação subsequente. Para a segurança dos nossos clientes, o UnitedHealth Group não divulgará, discutirá ou confirmará questões de segurança.

Notificação Pública

Para proteger os nossos clientes, o UnitedHealth Group solicita que os investigadores de segurança não publiquem ou compartilhem quaisquer informações sobre uma potencial vulnerabilidade em qualquer ambiente público até que tenhamos pesquisado, respondido e abordado a vulnerabilidade comunicada e informado os clientes e partes interessadas conforme for necessário. O tempo para resolver uma vulnerabilidade válida denunciada poderá variar com base no impacto da vulnerabilidade potencial e dos sistemas afetados.

Definições da Política

Vulnerabilidade: Uma fraqueza no design, implementação, operação ou controle interno de um processo que pode expor o sistema a ameaças adversas provenientes de eventos de ameaça.
Denial of Service (DoS): Um ataque a um serviço de uma única fonte que o inunda com tantas solicitações que ele fica sobrecarregado e é interrompido completamente ou opera a uma velocidade significativamente reduzida.
Distributed Denial of Service (DDoS): Um ataque a um serviço de vários sistemas de computador comprometidos que o inunda com tantas solicitações que ele fica sobrecarregado e é completamente interrompido ou opera a uma velocidade significativamente reduzida, negando assim o serviço a usuários ou sistemas legítimos.
Transport Layer Security (TLS): Um protocolo que fornece privacidade nas comunicações pela Internet. O protocolo permite que aplicativos cliente/servidor se comuniquem de uma forma projetada para evitar espionagem, adulteração ou falsificação de mensagens.
Self-Cross-Site Scripting (XCSS): Um ataque de engenharia social para obter controle das contas web de uma vítima por meio da execução inadvertida de código malicioso em seu próprio navegador.

Cross-Site Request Forgery (CSRF): Um tipo de exploração maliciosa de um site onde comandos não autorizados são transmitidos por um usuário no qual o site confia. Isso também é conhecido como ataque de clique único ou *session riding*.

Data de Entrada em Vigor

A data de entrada em vigor desta política é 20 de janeiro de 2023.