OBJECT FIRST

Relatório de teste

CISA Secure by Design Pledge

A Object First reforça seu compromisso

O que é Secure by Design?

A Cybersecurity and Infrastructure Security Agency (CISA) lidera o esforço nacional para entender, gerenciar e reduzir os riscos da nossa infraestrutura cibernética e física. Ela colabora com as partes interessadas da indústria e governo para fortalecerem sua própria segurança e resiliência. Como parte dos seus esforços, a CISA desenvolveu o Secure by Design Pledge. Este compromisso encoraja os fabricantes de software a melhorar voluntariamente a segurança dos seus produtos e serviços de software empresarial. O compromisso é estruturado em sete metas, cada uma com critérios que os fabricantes se comprometem a alcançar.

Os fabricantes são encorajados a demonstrar progresso mensurável na direção dessas metas em todos os seus produtos e para comunicar a conclusão de metas ou um roteiro para a conclusão. Se o fabricante atender ou exceder uma meta, ele é encorajado a descrever suas ações publicamente.

Este compromisso complementa e constrói sobre as melhores práticas de segurança de software desenvolvidas pela CISA, NIST, outras agências federais e as melhores práticas internacionais e do setor. Ele busca colocar uma postura "secure by design" no setor de software. A Object First está orgulhosa em assinar o compromisso Secure by Design da CISA. Nosso principal produto, o Ootbi, atualmente atende ou está em desenvolvimento para completar os critérios do compromisso. Nós acreditamos que é vital que todos os fornecedores façam o mesmo. Este documento irá destacar nosso progresso no sentido de atender aos critérios do Secure by Design Pledge.

© 2024 Object First. Todos os direitos reservados. Todas as marcas registradas são propriedade de seus respectivos donos. Erros e omissões excetuados.

Autenticação Multifator (MFA)

Meta da CISA

Dentro de um ano depois da assinatura do compromisso, demonstrar ações tomadas para aumentar mensuravelmente o uso de autenticação multifator em todos os produtos do fabricante.

Compromissos da Object First

A Object First já atende a esta meta. O Ootbi da Object First suporta configuração MFA, e nossas melhores práticas descrevem a configuração disso como parte do setup e configuração iniciais. O MFA pode ser habilitado no módulo de configuração na interface web de usuário do nosso produto.

Senhas Padrão

Meta da CISA

Dentro de um ano depois da assinatura do compromisso, demonstrar progresso mensurável no sentido de ter senhas padrão em todos os produtos do fabricante.

Compromissos da Object First

A Object First já atende a esta meta. Uma senha é usada durante a configuração inicial, gerada de forma única por aplicação e impressa na aba removível para conexão via IPMI. Durante a configuração, é solicitado que o usuário crie uma senha forte para todos os acessos futuros. Nenhuma senha padrão universal é usada.

Reduzir toda classe de Vulnerabilidade

Meta da CISA

Dentro de um ano depois da assinatura do compromisso, demonstrar ações tomadas no sentido de habilitar uma redução mensurável da prevalência de uma mais classes de vulnerabilidade em todos os produtos do fabricante.

Compromissos da Object First

A Object First contrata agências de teste terceirizadas para realizar testes de penetração para ajudar a encontrar e remediar lacunas de segurança. Por exemplo, durante testes no segundo trimestre de 2024, nós identificamos algumas lacunas durante testes e lançamos um patch Ootbi 1.5 para endereçá-las.

© 2024 Object First. Todos os direitos reservados. Todas as marcas registradas são propriedade de seus respectivos donos. Erros e omissões excetuados.

Patches de Segurança

Meta da CISA

Dentro de um ano depois da assinatura do compromisso, demonstrar ações tomadas para reduzir mensuravelmente a instalação de patches de segurança pelos clientes.

Compromissos da Object First

A Object First já atende a esta meta. A Object First lança continuamente patches de produto que endereçam o feedback dos clientes e descobertas sobre segurança. Quando atualizações estão disponíveis, nós notificamos os clientes diretamente por meio da IU do produto, se eles estiverem usando uma versão anterior. Nós buscamos garantir que todos os clientes estejam usando a versão mais recente quando possível, mas também reconhecemos que, realisticamente, isso não pode ser sempre monitorado ou aplicado, então definimos uma meta de que todos os clientes da Object First estejam usando o patch de segurança mais recente dentro de 30 dias após o lançamento.

Nós implementaremos um processo para ajudar a aumentar a adoção dos patches de segurança avaliando as versões atuais dos clientes por meio de telemetria de produto e então orquestrando um programa de acompanhamento em múltiplas etapas usando a Equipe de Sucesso do Cliente da Object First para ajudar a informar e encorajar a adoção da atualização.

Política de Divulgação de Vulnerabilidades

Meta da CISA

Dentro de um ano depois da assinatura do compromisso, publicar uma política de divulgação de vulnerabilidades (VDP) que autorize teste pelos membros do público em produtos oferecidos pelo fabricante, se comprometer a não recomendar ou buscar ação legal contra alguém realizando esforços de boa fé para seguir o VDP, fornecer um canal claro para reportar vulnerabilidades e permitir a divulgação pública de vulnerabilidades em linha com as melhores práticas e normas internacionais coordenadas de divulgação de vulnerabilidades.

Compromissos da Object First

A Object First já atende a esta meta. A política de divulgação de vulnerabilidades da Object First's está disponível no nosso site: https://objectfirst.com/legal/vulnerability-disclosure-policy/.

Qualquer pessoa que tenha identificado uma questão de segurança pode entrar em contato diretamente conosco pelo e-mail security@objectfirst.com.

© 2024 Object First. Todos os direitos reservados. Todas as marcas registradas são propriedade de seus respectivos donos. Erros e omissões excetuados.

CVEs

Meta da CISA

Dentro de um ano depois da assinatura do compromisso, demonstrar transparência no reporte de vulnerabilidades, incluindo campos Enumeração de Pontos Fracos Comuns (CWE) e Enumeração de Plataformas Comuns (CPE) em todo registro de Vulnerabilidades e Exposições Comuns (CVE) dos produtos do fabricante. Além disso, emitir CVEs em tempo hábil para, no mínimo, todas as vulnerabilidades críticas ou de alto impacto (sejam descobertas internamente ou por um terceiro) que exijam que um cliente tome ações para corrigir ou tenham evidências de exploração ativa.

Embora não seja requerido por esta meta, as empresas são encorajadas a ir acima e além, preenchendo CVEs para outras vulnerabilidades que não atendem a este critérios pelas razões descritas abaixo. As empresas também são encorajadas a explorar formas adicionais de enriquecer seus registros de CVE para ajudar os clientes a responder melhor a vulnerabilidades.

Compromissos da Object First

A Object First publicará um relatório de quaisquer Vulnerabilidades e Exposições Comuns (CVEs) em 2024.

Evidência de Intrusões

Meta da CISA

Dentro de um ano depois da assinatura do compromisso,demonstrar um aumento mensurável na habilidade dos clientes de reunir evidências de intrusões de segurança cibernética afetando os produtos do fabricante.

Compromissos da Object First

A Object First já atende a esta meta. e pacotes de suporte do Ootbi da Object First permitem aos usuários embalar e nos enviar quaisquer relatórios diretamente e com eficiência. Eles também podem criar um relatório por meio da VDP mencionada antes ou enviando um e-mail para security@objectfirst.com.

Saiba Mais

Os clientes da Veeam merecem uma solução que seja segura por projeto e priorize a resiliência dos dados. Visite a Object First para saber como o Ootbi (Out-of-the-Box Immutability) proporciona uma solução de backups segura, simples e potente que melhor protege os dados de backup da Veeam contra ameaças internas, ataques cibernéticos e ransomware.

© 2024 Object First. Todos os direitos reservados. Todas as marcas registradas são propriedade de seus respectivos donos. Erros e omissões excetuados.