
American Archive of Public Broadcasting corrige bug expondo mídia restr

Data: 2025-09-23 01:42:39

Autor: Inteligência Against Invaders

Uma vulnerabilidade no site do American Archive of Public Broadcasting permitiu o download de mídia protegida e privada por anos, com a falha silenciosamente corrigida este mês.

O BleepingComputer foi informado sobre a falha por um pesquisador de segurança cibernética que pediu para permanecer anônimo, afirmando que a falha foi explorada desde pelo menos 2021, mesmo depois que o pesquisador a relatou anteriormente à organização.

Depois de entrar em contato com a AAPB sobre a falha, um porta-voz confirmou o problema e o pesquisador validou que a correção foi implementada em 48 horas.

“Estamos comprometidos em proteger e preservar o material de arquivo na AAPB e fortalecemos a segurança do arquivo”, afirmou a gerente de comunicações da AAPB, Emily Balk, ao BleepingComputer.

“Estamos ansiosos para continuar a tornar a história da mídia pública gratuita e acessível ao público.”

O American Archive, operado pela WGBH Educational Foundation (GBH) e pela Biblioteca do Congresso, é um arquivo público sem fins lucrativos cuja missão é coletar, digitalizar e preservar conteúdo historicamente significativo produzido por rádio e televisão públicas nos Estados Unidos.

O BleepingComputer foi informado de que a vulnerabilidade AAPB circulou pela primeira vez como um boato em discussões online sobre o vazamento do episódio “Wicked Witch of the West” da Vila Sésamo no canal Discord da Lost Media Wiki.

O Lost Media Wiki retirou o episódio, dizendo que “provavelmente foi obtido em uma violação ilegal de dados”, pedindo aos membros que se abstenham de compartilhá-lo novamente em seu canal Discord.

Inicialmente secreto, o método de exploração começou a circular em grupos de preservação do Discord em meados de 2024, levando a novos vazamentos de conteúdo protegido em servidores Discord focados na preservação de conteúdo.

Conhecidas como acumuladores de dados, essas comunidades se dedicam ao arquivamento de software, sites, sistemas operacionais e várias formas de mídia, incluindo programas de TV, músicas e filmes. No entanto, eles geralmente operam em uma área cinzenta, onde o conteúdo protegido por direitos autorais é preservado e compartilhado, confundindo a linha com a pirataria digital.

Mesmo com os esforços de remoção da AAPB, o exploit continuou a circular em vários servidores

Discord e aplicativos de mensagens, com uma prova de conceito compartilhada com o BleepingComputer mostrando como era fácil abusar.

O exploit compartilhado com o BleepingComputer é um script Tampermonkey simples que explora uma falha insegura de referência direta de objeto (IDOR), permitindo que os usuários solicitem arquivos de mídia por ID e ignorem os controles de acesso do AAPB.

O bug permitiu que os usuários alterassem o parâmetro de ID de mídia em solicitações de acesso à mídia, permitindo que eles acessassem recursos pelo ID, mesmo que fossem protegidos ou privados.

Embora as páginas principais /media/{ID} tivessem alguns controles de acesso, os invasores podiam ignorá-los adulterando as chamadas fetch ou XMLHttpRequest feitas em segundo plano.

Em vez de o servidor da AAPB rejeitar essas solicitações com um erro '403 Forbidden', desde que a solicitação tivesse um ID de mídia válido, o conteúdo foi veiculado.

Embora a vulnerabilidade tenha sido corrigida, não se sabe quanto conteúdo foi acessado e compartilhado na comunidade de acumuladores de dados.

O vazamento de conteúdo no American Archive seguiu outro incidente no início deste ano, onde [As informações de contato dos funcionários da PBS vazaram](#) e se espalhou pelos servidores Discord para os fãs de 'PBS Kids'.

Ambos os incidentes ilustram como as comunidades de arquivos e fãs podem obter acesso a dados confidenciais ou privados, mesmo quando não são usados para fins maliciosos.

[\[IMAGEM REMOVIDA\]](#)

-