

ステータス:	終了	開始日:	2021/03/18
優先度:	通常	期日:	
担当者:	菊池 威之	進捗率:	100%
カテゴリ:		予定工数:	3.00時間
機能名:	雇用契約一括ダウンロード	要マニュアル反映:	いいえ
原因区分:	脆弱性診断		
説明			
指摘事項			
危険度			
低			
解説			
遷移先を指定するHTML タグ属性のホスト名にホストヘッダの値が使用されていることが確認されました。ホストヘッダの値を改ざんすることにより、被害者を任意のホストへアクセスさせることが可能です。また、CSS のURL が改ざんされる箇所では、CSS インジェクションを利用したサイトの改ざん等の攻撃、JavaScript のURL が改ざんされる箇所では任意のスクリプトをインポートすることが可能です。ただし、第三者によるホストヘッダの改ざんは大変困難であるため、本事項が悪用される可能性は極めて低いと思われます。			
検出箇所 URL			
https://c.economic-app.com/ecclub/KoyouKeiyakushoIkatsuDownLoad/KoyouKeiyakushodownload/search			
回答・対応内容			
事象			
ページングのURLが改ざんしたホストの影響を受けてしまう。			
対応内容			
下記のようにペジネーターURIをカスタマイズする。			
->paginate(100); を ->paginate(100)->withPath(""); へ変更			
他、確認したアクション			
ソート いいねボタン 添付ファイルダウンロード メール送信 CSV/PDFダウンロード			

バリデーションエラー

詳細は添付ファイル参照

対応確認いたしました。

履歴

- #1 - 2021/03/18 13:10 - 匿名ユーザー
- 回答・対応内容 を更新
- 題名 を [脆弱性診断]ホストヘッダによるリンクの改ざん から [脆弱性診断]ホストヘッダによるリンクの改ざん ページングに変更
- #2 - 2021/03/18 13:10 - 匿名ユーザー
- 回答・対応内容 を更新
- #3 - 2021/03/18 13:12 - 匿名ユーザー
- 担当者 を 匿名ユーザー から 菊池 威之 に変更
- ステータス を 新規 から 承認済に変更
- #4 - 2021/03/18 13:15 - 匿名ユーザー
- ステータス を 承認済 から 対応済に変更
- #5 - 2021/03/23 01:42 - 匿名ユーザー
- 回答・対応内容 を更新
- ファイル [指摘事項 #174]確認操作.xlsx を追加
- #6 - 2021/03/24 04:53 - 菊池 威之
- ステータス を 対応済 から 終了に変更

再診断にてOKができましたので、クローズします。

ファイル

[指摘事項 #174]確認操作.xlsx	13.4 KB	2021/03/23	匿名ユーザー
----------------------	---------	------------	--------