

受入試験（指摘事項管理） - 指摘事項 #167

[脆弱性診断]ホストヘッダによるリンクの改ざん

2021/03/04 08:24 - 匿名ユーザー

ステータス:	終了	開始日:	2021/03/04
優先度:	通常	期日:	
担当者:		進捗率:	100%
カテゴリ:		予定工数:	2.00時間
機能名:	全般	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.ecomic-app.com/ecclub/eco/ecnews/henshu https://c.ecomic-app.com/ecclub/eco/ecnews/toukouichiran https://c.ecomic-app.com/ecclub/eco/ecnews/touroku https://c.ecomic-app.com/ecclub/jugyoin/henshu https://c.ecomic-app.com/ecclub/jugyoin/ichiran https://c.ecomic-app.com/ecclub/jugyoin/ichiran/kensaku https://c.ecomic-app.com/ecclub/jugyoin/kaishaSentaku https://c.ecomic-app.com/ecclub/jugyoin/pasuwado https://c.ecomic-app.com/ecclub/jugyoin/settei https://c.ecomic-app.com/ecclub/jugyoin/settei/kakunin https://c.ecomic-app.com/ecclub/kyuyokokaibi https://c.ecomic-app.com/ecclub/kyuyokokaibidetail/nextMonth https://c.ecomic-app.com/ecclub/kyuyokokaibidetail/preMonth https://c.ecomic-app.com/ecclub/kyuyokokaibidetail/showdetail https://c.ecomic-app.com/ecclub/login https://c.ecomic-app.com/ecclub/pasuwado https://c.ecomic-app.com/ecclub/portal https://c.ecomic-app.com/ecclub/portalKaishaSentaku https://c.ecomic-app.com/ecclub/portalKaishaSentaku/kensaku https://c.ecomic-app.com/ecclub/roru https://c.ecomic-app.com/ecclub/shain https://c.ecomic-app.com/ecclub/shain/upload https://c.ecomic-app.com/ecclub/KoyouKeiyakushoIkatsuDownLoad/KoyouKeiyakushodownload/search https://c.ecomic-app.com/ecclub/KoyouKeiyakushoIkatsuDownLoad/KoyouKeiyakushodownload/show https://c.ecomic-app.com/ecclub/koyouKeiyakusyoTenpuretoUpload/ichiran https://c.ecomic-app.com/ecclub/koyouKeiyakusyoUpload https://c.ecomic-app.com/ecclub/koyouKeiyakusyoUpload/upload https://c.ecomic-app.com/ecclub/koyoukeiyakushokansadownload https://c.ecomic-app.com/ecclub/koyoukeiyakushokansadownload/download https://c.ecomic-app.com/ecclub/koyoukeiyakusho/handleformall			

<https://c.economic-app.com/ecclub/koyoukeiyakusho/ichiran>
<https://c.economic-app.com/ecclub/kyoten/henshu>
<https://c.economic-app.com/ecclub/kyoten/kanrisha>
<https://c.economic-app.com/ecclub/kyoten/kanrisha/tsuika>
<https://c.economic-app.com/ecclub/kyuyoMeisaiChiran/selectYear>
<https://c.economic-app.com/ecclub/kyuyoMeisaiSho>
<https://c.economic-app.com/ecclub/kyuyoMeisaiSho/changeMonth>
<https://c.economic-app.com/ecclub/dokumento/ichiran>

回答・対応内容

URLジェネレーターで、設定ファイルに指定したホスト名を使用する。

・検証環境

<https://albec-1244903380.ap-northeast-1.elb.amazonaws.com>

・本番環境

<https://c.economic-app.com>

→対応後の確認結果を添付

対応確認いたしました。

履歴

#1 - 2021/03/04 08:29 - 匿名ユーザー

- 指摘事項を更新

#2 - 2021/03/04 08:32 - 匿名ユーザー

- 指摘事項を更新

#3 - 2021/03/04 08:36 - 匿名ユーザー

- 回答・対応内容を更新

#4 - 2021/03/04 12:07 - 匿名ユーザー

- 予定工数を 2.00時間 にセット

#5 - 2021/03/05 03:48 - 菊池 威之

- ステータスを 新規 から 対応中 に変更

#6 - 2021/03/05 08:25 - 匿名ユーザー

- 担当者を 匿名ユーザー から 拓圭 深田 に変更

- 進捗率を 0 から 100 に変更

- ステータスを 対応中 から 対応済 に変更

#7 - 2021/03/08 02:59 - 匿名ユーザー

- 回答・対応内容を更新

- ファイル 対応後確認_指摘事項 #167 [脆弱性診断]ホストヘッダによるリンクの改ざん.xlsx を追加

#8 - 2021/03/08 10:16 - 匿名ユーザー

- ファイルを削除 (対応後確認_指摘事項 #167 [脆弱性診断]ホストヘッダによるリンクの改ざん.xlsx)

- ファイル 対応後確認_指摘事項 #167 [脆弱性診断]ホストヘッダによるリンクの改ざん.xlsx を追加

#9 - 2021/03/09 01:43 - 拓圭 深田

- 回答・対応内容を更新

- 担当者を 拓圭 深田 から 菊池 威之 に変更

- ステータスを 対応済 から 承認済 に変更

#10 - 2021/03/10 03:37 - 菊池 威之

- 担当者を 菊池 威之 から 匿名ユーザー に変更

#11 - 2021/03/18 12:41 - 菊池 威之

- ステータスを 承認済 から 終了 に変更

再診断結果OKにてクローズします。

ファイル

対応後確認_指摘事項 #167 [脆弱性診断]ホストヘッダによるリンクの改ざん.xlsx 2021/03/08

匿名ユーザー