2016 年 2 月 29 日

(改訂日 : 2016 年 3 月 9 日)

※改訂履歴は最終ページに記載

お客様各位

株式会社セゾン情報システムズ

HULFT 事業部

HULFT Series 製品における glibc ライブラリの脆弱性(CVE-2015-7547)に対する報告

HULFT Series 製品における glibc ライブラリの脆弱性(CVE-2015-7547)に対する報告をご案内いたします。

― 記 ―

1. 脆弱性の内容

glibc ライブラリにおいて、重大な脆弱性が公表されました (CVE-2015-7547)。この脆弱性を悪用された場合、遠隔の第三者によって任意のコードを実行されたり、サービス運用妨害(DoS)攻撃が行われたりする可能性があります。

<glibc ライブラリの脆弱性に関する情報>
http://www.jpcert.or.jp/at/2016/at160009.html

2. 調査状況

上記脆弱性について HULFT Series 製品における影響をご案内いたします。
<HULFT Series 製品 調査状況 - 2016 年 3 月 7 日 9:00 時点>

製品名	調査状況
HULFT	Linux 版で影響があります。影響を受けるのは以下の条件すべてに該当する場合です。 ・お客様環境に導入されている glibc のバージョンが 2.9 以降の場合 ・システム動作環境設定にて"ipversion"が"4"以外に設定されている場合 ・ホスト名解決に DNS を使用する環境で製品をご利用の場合 上記条件に該当する場合、glibc の修正済バージョンを適用し、当該製品を再起動してください。
HULFT BB	影響ありません。
HULFT8 Script Option	Linux 版で影響があります。影響を受けるのは以下の条件すべてに該当する場合です。 ・お客様環境に導入されている glibc のバージョンが 2.9 以降の場合 ・ホスト名解決に DNS を使用する環境で製品をご利用の場合 ・IPv6 を使用する環境でご利用の場合 上記条件に該当する場合、glibc の修正済バージョンを適用し、当該製品を再起動してください。

HULFT-HUB	影響ありません。
HULFT-DataMagic	Linux 版で影響があります。影響を受けるのは以下の条件すべてに該当する場合です。 ・お客様環境に導入されている glibc のバージョンが 2.9 以降の場合 ・ホスト名解決に DNS を使用する環境で製品をご利用の場合 上記条件に該当する場合、glibc の修正済バージョンを適用し、当該製品を再起動してください。
HULFT-WebFT	Linux 環境にてご利用中で、以下の条件すべてに該当する場合に影響があります。 ・お客様環境に導入されている glibc のバージョンが 2.9 以降の場合 ・ホスト名解決に DNS を使用する環境で製品をご利用の場合 ・IPv6 を使用する環境でご利用の場合 上記条件に該当する場合、glibc の修正済バージョンを適用し、当該製品を再起動してください。
HULFT-WebConnect	Linux 環境にて HULFT-WebConnect Agent をご利用中で、以下の条件すべてに該当する場合に影響があります。 ・お客様環境に導入されている glibc のバージョンが 2.9 以降の場合 ・IPv6 を使用する環境でご利用の場合 上記条件に該当する場合、glibc の修正済バージョンを適用し、当該製品を再起動してください。
HDC-EDI Suite	Linux 環境にてご利用中で、以下の条件すべてに該当する場合に影響があります。 ・お客様環境に導入されている glibc のバージョンが 2.9 以降の場合 ・ホスト名解決に DNS を使用する環境で製品をご利用の場合 ・IPv6 を使用する環境でご利用の場合 上記条件に該当する場合、glibc の修正済バージョンを適用し、当該製品を再起動してください。
iDIVO	Linux 版で影響があります。影響を受けるのは以下の条件すべてに該当する場合です。 ・お客様環境に導入されている glibc のバージョンが 2.9 以降の場合 ・ホスト名解決に DNS を使用する環境で製品をご利用の場合 上記条件に該当する場合、glibc の修正済バージョンを適用し、当該製品を再起動してください。
SIGNAlert	影響ありません。

【改訂履歴】

2016 年 2 月 29 日	初版作成
2016 年 3 月 9 日	下記製品の調査状況に、影響を受ける条件を追記しました。 HULFT-WebFT HULFT-WebConnect HDC-EDI Suite

以上