

HA8500 シリーズ における iLO の脆弱性(CVE-2020-11906 他)について

1. 脆弱性の内容

iLO の IP スタックに複数の脆弱性がみつけられました。これらの脆弱性により、サービス運用妨害 (DoS)などの攻撃を iLO が受ける可能性があります。対象製品、および詳細は、次項に記載の対象製品、および CVE を参照してください。

2. 対象製品

| 製品名 | モデル | CVE | 影響を受ける Firmware | 対策版 Firmware |
|----------------------------|----------------------|--|-----------------|-----------------|
| 日立アドバンストサーバ HA8500 シリーズ | SDE6 SDF7 SDF8 | CVE-2020-11906 CVE-2020-11907 CVE-2020-11911 | バージョン v20.02 以前 | バージョン v21.03 以降 |
| | 310E6 | | バージョン v20.02 以前 | バージョン v21.11 以降 |
| | 310F7 310F8 | | バージョン v20.02 以前 | バージョン v21.06 以降 |
| | BL8x0F7 BL8x0F8 | | バージョン v20.04 以前 | バージョン v21.09 以降 |

* 上記のリンクのいずれかをクリックすると、Hitachi, Ltd.以外の Web サイトが表示されます。

Hitachi は、Hitachi 外部の Web サイトの情報を管理しておらず、また、それらに関する責任も負いません。

3. 対策方法

ファームウェアを対策バージョンにアップデートしてください。

対策版ファームウェアへのアップデートは保守員が実施しますので、アップデートをご希望される場合は、製品サポート窓口にお問合せください。

4. お問い合わせ先

製品サポート窓口にお問合せください。

5. 更新情報

2022年2月9日：310E6, BL8x0F7, BL8x0F8 モデルの情報を追加しました。

2021年7月19日：310F7, 310F8 モデルの情報を追加しました。

2021年6月1日：このセキュリティ情報ページを新規作成および発信しました。

- 弊社では、セキュリティ対応に関して正確な情報を提供できるよう努力しておりますが、セキュリティ問題に関する情報は変化しており、当ホームページで記載している内容を予告なく変更することがありますので、あらかじめご了承ください。情報ご参照の際には、常に最新の情報をご確認いただくようお願いいたします。
- 当ホームページに記載されている製品には、他社開発製品が含まれております。これらのセキュリティ情報については他社から提供、または公開された情報を基にしております。弊社では、情報の正確性および完全性について注意を払っておりますが、開発元の状況変化に伴い、当ホームページの記載内容に変更が生じることがあります。
- 当ホームページはセキュリティ情報の提供を目的としたものであり、法律上の責任を負うものではありません。お客様が独自に行なった(あるいは行なわなかった)セキュリティ対応その他のご行為の結果につきまして、弊社では責任を負いかねます。
- 当ホームページから他サイトのページへのリンクアドレスは情報発信時のものです。他サイトでの変更などを発見した場合には、リンク切れ等にならないように努力はいたしますが、永続的にリンク先を保証するものではありません。