2021 年 3 月 18 日
株式会社ネットワールド

CVE-2021-22986, CVE-2021-22987, CVE-2021-22991, CVE-2021-22992
F5 critical vulnerabilities (2021/03)に関する脆弱性公開／対策のお知らせ

4 件の BIG-IP/BIG-IQ の Severity「Critical」な脆弱性について、メーカーサイト「AskF5」上で対策を含めた詳細情報が公開されております。

不具合が修正されている OS バージョンへのバージョンアップを強く推奨しておりますので内容をご一読の上、対策の実施をご検討頂けますようお願いいたします。

1.CVE-2021-22986 - K03009991

SOL 番号	K03009991
URL	https://support.f5.com/csp/article/K03009991
タイトル	iControl REST Unauthenticated remote command execution vulnerability CVE-2021-22986
関連 CVE	CVE-2021-22986
公開日	2021 年 3 月 10 日 米国時間
脆弱性概要	通常リモートからマネージメントポートもしくは SelfIP を経由し iControl REST インターフェースにアクセスする場合は、ユーザ認証が必要ですが、今回の脆弱性によりユーザ認証無しに任意のコード実行、ファイル作成・削除、サービスの無効化などを実行される恐れがあります。
一時的な軽減策の有無	有
恒久対策の有無	有
備考	この脆弱性は Control Plane のみが対象となります。

2.CVE-2021-22987 - K18132488

SOL 番号	K18132488
URL	https://support.f5.com/csp/article/K18132488
タイトル	Appliance Mode TMUI Authenticated remote command execution vulnerability CVE-2021-22987
関連 CVE	CVE-2021-22987
公開日	2021 年 3 月 10 日米国時間

脆弱性概要	Appliance Mode で稼働している場合に、マネージメントポートもしくは SelfIP を経由し Configuration Utility に認証してアクセス可能なユーザにて、今回の脆弱性により K12815 に記載された Appliance Mode での制限を超えて任意のコード実行、ファイル作成・削除、サービスの無効化などを実行される恐れがあります。
一時的な軽減策の有無	有
恒久対策の有無	有
備考	この脆弱性は Control Plane のみが対象となります。Appliance Mode は特定の License の適用もしくは vCMP ゲスト上で Enabled した場合のみ動作します。

3.CVE-2021-22991 - K56715231

SOL 番号	K56715231
URL	https://support.f5.com/csp/article/K56715231
タイトル	TMM Buffer Overflow vulnerability CVE-2021-22991
関連 CVE	CVE-2021-22991
公開日	2021 年 3 月 10 日米国時間
脆弱性概要	第三者が悪意のあるリクエストを Virtual Server へ送ることにより、TMM で URI 正規化を行った際にバッファオーバーフローが発生する可能性があり、結果として DoS 攻撃が可能となります。これにより URL ベースでのアクセス制御を無視したり、Remote Code Execution が実行可能であるという問題です。
一時的な軽減策の有無	無
恒久対策の有無	有
備考	この脆弱性は Data Plane のみが対象となります。該当プロダクト情報等詳細は上記 SOL をご参照ください。

4.CVE-2021-22992 - K52510511

SOL 番号	K52510511
URL	https://support.f5.com/csp/article/K52510511
タイトル	Advanced WAF/ASM Buffer Overflow vulnerability CVE-2021-22992
関連 CVE	CVE-2021-22992
公開日	2021 年 3 月 10 日米国時間
脆弱性概要	BIG-IP Advanced WAF/ASM の Virtual Server を設定しており、Login Page の設定がされている場合、特定の HTTP Response を処理した際に、バッファオーバーフローが発生し、結果として DoS 攻撃が可能となります。これにより、Remote Code Execution が実行可能であるという問題です。
一時的な軽減策の有無	有

恒久対策の有無	有
備考	この脆弱性は Data Plane のみが対象となります。Backend Server が特定の HTTP Response を返せる状態になっている場合のみとなります。

AskF5 での情報公開のほか、F5 ブログでも記載されております（日本語）
https://www.f5.com/ja_jp/company/blog/20210311cve

■問い合わせ窓口
弊社保守締結ユーザー様：TEC-World
https://tec-world.networld.co.jp/login

メーカー保守締結ユーザー様：F5 カスタマーサポートサービス窓口
https://www.f5.com/ja_jp/services/support/jp-support

以上