

重要度	発行日	アドバイザリ ID	関連セキュリティ勧告	タイトル	保護機能設定方法
緊急	2022年10月30日	CPAI-2022-0762	CVE-2022-2135	Advantech iView の SQL インジェクション (CVE-2022-2135)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Advantech iView SQL Injection (CVE-2022-2135)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年10月30日	CPAI-2022-0725	CVE-2022-25076 CVE-2022-25078 CVE-2022-25079 CVE-2022-25080 CVE-2022-25081 CVE-2022-25082 CVE-2022-25083 CVE-2022-25084	TOTOLink A860R のコマンドインジェクション (CVE-2022-25076; CVE-2022-25078; CVE-2022-25079; CVE-2022-25080; CVE-2022-25081; CVE-2022-25082; CVE-2022-25083; CVE-2022-25084)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [TOTOLink A860R Command Injection] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年10月30日	CPAI-2022-0759	CVE-2022-2139	Advantech iView のディレクトリトラバース (CVE-2022-2139)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Advantech iView Directory Traversal (CVE-2022-2139)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年10月31日	CPAI-2022-0727	CVE-2022-23389	PublicCMS のリモートからコードを実行される脆弱性 (CVE-2022-23389)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [PublicCMS Remote Code Execution (CVE-2022-23389)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年10月31日	CPAI-2021-1329	CVE-2021-2394	Oracle WebLogic Server のリモートからコードを実行される脆弱性 (CVE-2021-2394)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Oracle WebLogic Server Remote Code Execution (CVE-2021-2394)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年10月31日	CPAI-2020-3608	CVE-2020-17132	Microsoft Exchange のリモートからコードを実行される脆弱性 (CVE-2020-17132)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Microsoft Exchange Remote Code Execution (CVE-2020-17132)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年10月31日	CPAI-2022-0766	CVE-2022-2143	Advantech iView のコマンドインジェクション (CVE-2022-2143)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Advantech iView Command Injection (CVE-2022-2143)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年10月31日	CPAI-2022-0767	CVE-2022-1366	Delta Electronics DIAnergie の SQL インジェクション (CVE-2022-1366)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Delta Electronics DIAnergie SQL Injection (CVE-2022-1366)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月2日	CPAI-2022-0731	CVE-2022-0888	WordPress Ninja Forms プラグインで任意のファイルがアップロードされる脆弱性 (CVE-2022-0888)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [WordPress Ninja Forms Plugin Arbitrary File Upload (CVE-2022-0888)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月2日	CPAI-2022-0738	CVE-2022-33171	TypeORM FindOne で認証が回避される脆弱性 (CVE-2022-33171)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [TypeORM FindOne Authentication Bypass (CVE-2022-33171)] 保護機能を探し、保護機能の設定を編集します。

重要度	発行日	アドバイザリ ID	関連セキュリティ勧告	タイトル	保護機能設定方法
緊急	2022年11月2日	CPAI-2022-0741	CVE-2022-24223	AtomCMS の SQL インジェクション (CVE-2022-24223)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [AtomCMS SQL Injection (CVE-2022-24223)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月3日	CPAI-2022-0749	CVE-2022-29337	C-DATA のコマンドインジェクション (CVE-2022-29337)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [C-DATA Command Injection (CVE-2022-29337)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月3日	CPAI-2022-0779	CVE-2022-34555	TP-Link TL-R473G のコマンドインジェクション (CVE-2022-34555)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [TP-Link TL-R473G Command Injection (CVE-2022-34555)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月3日	CPAI-2022-0794	CVE-2022-23221	H2 Database のリモートからコードを実行される脆弱性 (CVE-2022-23221)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [H2 Database Remote Code Execution (CVE-2022-23221)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月3日	CPAI-2022-0785	CVE-2022-3786	OpenSSL のバッファ オーバーフロー (CVE-2022-3786)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [OpenSSL Buffer Overflow (CVE-2022-3786)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年5月24日	CPAI-2022-0243	CVE-2022-1040	Sophos MR3 ファイアウォールでリモートからコードを実行される脆弱性 (CVE-2022-1040)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Sophos MR3 Firewall Remote Code Execution (CVE-2022-1040)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月6日	CPAI-2022-0780	CVE-2022-34531	DedeCMS のコマンドインジェクション (CVE-2022-34531)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [DedeCMS Command Injection (CVE-2022-34531)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年5月19日	CPAI-2022-0251	CVE-2022-30525	Zyxel USG のコマンドインジェクション (CVE-2022-30525)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Zyxel USG Command Injection (CVE-2022-30525)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月6日	CPAI-2019-2674	CVE-2019-9165	Nagios XI の SQL インジェクション (CVE-2019-9165)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Nagios XI SQL Injection (CVE-2019-9165)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月6日	CPAI-2022-0683	CVE-2022-35914	GLPI Project のコードインジェクション (CVE-2022-35914)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [GLPI Project Code Injection (CVE-2022-35914)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月6日	CPAI-2022-0754	CVE-2022-29592	Tenda TX9 Pro ルータのコマンドインジェクション (CVE-2022-29592)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Tenda TX9 Pro Router Command Injection (CVE-2022-29592)] 保護機能を探し、保護機能の設定を編集します。