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10日	CPAI-2022-0800	CVE-2022-26990 CVE-2022-26991 CVE-2022-26992 CVE-2022-26993 CVE-2022-26994 CVE-2022-26995 CVE-2022-26996 CVE-2022-26997 CVE-2022-26998 CVE-2022-26999 CVE-2022-27000 CVE-2022-27001 CVE-2022-27002	Arris ルータのコマンドインジェクション (CVE-2022-26990; CVE-2022-26991; CVE-2022-26992; CVE-2022-26993; CVE-2022-26994; CVE-2022-26995; CVE-2022-26996; CVE-2022-26997; CVE-2022-26998; CVE-2022-26999; CVE-2022-27000; CVE-2022-27001; CVE-2022-27002)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Arris Routers 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11月17日	CPAI-2022-0856	CVE-2022-22916	O2OA でリモートからコードを実行される脆弱性 (CVE-2022-22916)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［O2OA Remote Code Execution (CVE-2022-22916)］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17日	CPAI-2021-1376	CVE-2021-40493	Zoho ManageEngine の SQL インジェクション (CVE-2021-40493)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Zoho ManageEngine SQL Injection (CVE-2021-40493)］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17日	CPAI-2022-0805	CVE-2022-35411	rpc.py プロジェクトでリモートからコードを実行される脆弱性 (CVE-2022-35411)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［rpc.py Project Remote Code Execution (CVE-2022-35411)］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17日	CPAI-2022-0857	CVE-2022-3218	Necta LLC WiFi マウスのコマンドインジェクション (CVE-2022-3218)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Necta LLC WiFi Mouse Command Injection (CVE-2022-3218)］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17日	CPAI-2017-1537	CVE-2017-17420	Quest NetVault Backup NVBUJobCountHistory の SQL インジェクション (CVE-2017-17420)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Quest NetVault Backup NVBUJobCountHistory SQL Injection (CVE-2017-17420)］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17日	CPAI-2018-2149	CVE-2018-7890	Zoho ManageEngine ApplicationManager のコマンドインジェクション (CVE-2018-7890)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Zoho ManageEngine ApplicationManager Command Injection (CVE-2018-7890)］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17日	CPAI-2022-0818	CVE-2022-27336	Seacms のリモートからコードを実行される脆弱性 (CVE-2022-27336)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Seacms Remote Code Execution (CVE-2022-27336)］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17日	CPAI-2021-1366	CVE-2021-41950	Montala Limited ResourceSpace で任意のファイルが削除される脆弱性 (CVE-2021-41950)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Montala Limited ResourceSpace Arbitrary File Deletion (CVE-2021-41950)］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17日	CPAI-2022-0849	CVE-2022-26833	Open Automation Software プラットフォームで認証が回避される脆弱性 (CVE-2022-26833)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Open Automation Software Platform Authentication Bypass (CVE-2022-26833)］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20日	CPAI-2019-2683	CVE-2019-16724	iSharer および upRedSun ファイル共有ウィザードのバッファ オーバーフロー (CVE-2019-16724)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［iSharer and upRedSun File Sharing Wizard Buffer Overflow (CVE-2019-16724)］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20日	CPAI-2022-0862	CVE-2022-23900	Wavlink WL-WN531P3 のコマンドインジェクション (CVE-2022-23900)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Wavlink WL-WN531P3 Command Injection (CVE-2022-23900)］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21日	CPAI-2022-0910	CVE-2022-29013	Razer Sila ゲーム向けルータのコマンドインジェクション (CVE-2022-29013)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Razer Sila Gaming Router Command Injection (CVE-2022-29013)］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21日	CPAI-2022-0919	CVE-2022-26960	Studio42 elFinder のディレクトリ トラバーサル (CVE-2022-26960)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Studio42 elFinder Directory Traversal (CVE-2022-26960)］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-2022-0781	CVE-2022-26501	Veeam バックアップおよび複製で認証が回避される脆弱性 (CVE-2022-26501)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Veeam Backup and Replication Authentication Bypass (CVE-2022-26501)］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21日	CPAI-2022-0897	CVE-2022-37061	FLIR AX8 サーモグラフィカメラのコマンドインジェクション (CVE-2022-37061)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［FLIR AX8 Thermal Camera Command Injection (CVE-2022-37061)］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21日	CPAI-2022-0868	CVE-2022-24108	OpenCart でリモートからコードを実行される脆弱性 (CVE-2022-24108)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［OpenCart Remote Code Execution (CVE-2022-24108)］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22日	CPAI-2022-0866	CVE-2022-24148 CVE-2022-24150	Tenda AX3 ルータのコマンドインジェクション (CVE-2022-24148; CVE-2022-24150)	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 AX3 Router 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11月22日	CPAI-2022-0885	CVE-2022-29307	IonizeCMS のコマンドインジェクション (CVE-2022-29307)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［IonizeCMS Command Injection (CVE-2022-29307)］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22日	CPAI-2022-0888	CVE-2022-25061	TP-Link TL-WR840N のコマンドインジェクション (CVE-2022-25061)	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-WR840N Command Injection (CVE-2022-25061)］保護機能を探し、保護機能の設定を編集します。