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	2024年7月23日	CPAI-2024-0602	CVE-2024-0986	Issabel PBX のコマンド インジェクション (CVE-2024-0986)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Issabel PBX Command Injection (CVE-2024-0986)］保護機能を探し、保護機能の設定を編集します。
緊急	2024年6月20日	CPAI-2024-0416	CVE-2024-23692	Rejetto HTTP File Server のサーバサイド テンプレート インジェクション (CVE-2024-23692)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Rejetto HTTP File Server Server-Side Template Injection (CVE-2024-23692)］保護機能を探し、保護機能の設定を編集します。
緊急	2024年7月24日	CPAI-2024-0587	CVE-2024-27172	東芝のマルチファンクションプリンターに発見されたコマンド インジェクションの脆弱性 (CVE-2024-27172)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Toshiba Multi-Function Printers Command Injection (CVE-2024-27172)］保護機能を探し、保護機能の設定を編集します。
緊急	2024年3月3日	CPAI-2024-0034	CVE-2020-9437	クライアントサイド テンプレート インジェクション (CVE-2020-9437)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Client-Side Template Injection (CVE-2020-9437)］保護機能を探し、保護機能の設定を編集します。
緊急	2024年4月2日	CPAI-2023-1623	CVE-2022-32039 CVE-2022-32040 CVE-2022-32043 CVE-2023-37710 CVE-2023-37714 CVE-2023-37715 CVE-2023-37716 CVE-2023-37717 CVE-2023-37718 CVE-2023-37719 CVE-2023-37721 CVE-2023-37722 CVE-2023-37723 CVE-2023-51093	Tenda の複数製品に発見されたスタック オーバーフロー (CVE-2022-32039; CVE-2022-32040; CVE-2022-32043; CVE-2023-37710; CVE-2023-37714; CVE-2023-37715; CVE-2023-37716; CVE-2023-37717; CVE-2023-37718; CVE-2023-37719; CVE-2023-37721; CVE-2023-37722; CVE-2023-37723; CVE-2023-51093)	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 Multiple Products Stack Overflow］保護機能を探し、保護機能の設定を編集します。
緊急	2024年7月28日	CPAI-2023-1848	CVE-2023-37145 CVE-2023-37148	TOTOLINK LR350 のコマンド インジェクション (CVE-2023-37145; CVE-2023-37148)	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 LR350 Command Injection］保護機能を探し、保護機能の設定を編集します。
緊急	2024年7月28日	CPAI-2024-0606	CVE-2024-1651	Torrentpier の安全でないデシリアライズ (CVE-2024-1651)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Torrentpier Insecure Deserialization (CVE-2024-1651)］保護機能を探し、保護機能の設定を編集します。
緊急	2024年7月28日	CPAI-2023-1851	CVE-2023-1698	WAGO のコマンド インジェクション (CVE-2023-1698)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［WAGO Command Injection (CVE-2023-1698)］保護機能を探し、保護機能の設定を編集します。
緊急	2024年7月28日	CPAI-2023-1852	CVE-2023-34600	Adiscon LogAnalyzer の SQL インジェクション (CVE-2023-34600)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Adiscon LogAnalyzer SQL Injection (CVE-2023-34600)］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	2024年7月29日	CPAI-2024-0578	CVE-2024-27144 CVE-2024-27145 CVE-2024-27146 CVE-2024-27147 CVE-2024-27148 CVE-2024-27149 CVE-2024-27150 CVE-2024-27151 CVE-2024-27171	東芝のマルチファンクションプリンターに発見されたファイルの無制限アップロード (CVE-2024-27144; CVE-2024-27145; CVE-2024-27146; CVE-2024-27147; CVE-2024-27148; CVE-2024-27149; CVE-2024-27150; CVE-2024-27151; CVE-2024-27171)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Toshiba Multi-Function Printers Unrestricted File Upload］保護機能を探し、保護機能の設定を編集します。
緊急	2024年7月29日	CPAI-2018-2779	CVE-2018-1000517	BusyBox のバッファ オーバーフロー (CVE-2018-1000517)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［BusyBox Buffer Overflow (CVE-2018-1000517)］保護機能を探し、保護機能の設定を編集します。
緊急	2024年7月21日	CPAI-2024-0589	CVE-2024-4879 CVE-2024-5178 CVE-2024-5217	ServiceNow のサーバサイド テンプレート インジェクション (CVE-2024-4879; CVE-2024-5178; CVE-2024-5217)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［ServiceNow Server-Side Template Injection］保護機能を探し、保護機能の設定を編集します。
緊急	2024年7月30日	CPAI-2023-1850	CVE-2023-27076	Tenda G103 のコマンド インジェクション (CVE-2023-27076)	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 G103 Command Injection (CVE-2023-27076)］保護機能を探し、保護機能の設定を編集します。
緊急	2024年7月31日	CPAI-2023-1832	CVE-2023-43795	Osgeo GeoServer のサーバサイド リクエスト フォージェリ (CVE-2023-43795)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Osprey Pump Controller Command Injection］保護機能を探し、保護機能の設定を編集します。
緊急	2024年7月4日	CPAI-2023-1811	CVE-2023-27394 CVE-2023-28712	Osprey Pump Controller のコマンド インジェクション (CVE-2023-27394; CVE-2023-28712)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Osprey Pump Controller Command Injection］保護機能を探し、保護機能の設定を編集します。
緊急	2024年8月1日	CPAI-2023-1857	CVE-2023-30194	Prestashop Posthemes の SQL インジェクション (CVE-2023-30194)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Prestashop Posthemes SQL Injection (CVE-2023-30194)］保護機能を探し、保護機能の設定を編集します。
緊急	2024年7月25日	CPAI-2024-0614	CVE-2024-41110	Docker Engine に発見された認証バイパスの脆弱性 (CVE-2024-41110)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Docker Engine Authentication Bypass (CVE-2024-41110)］保護機能を探し、保護機能の設定を編集します。
緊急	2024年8月5日	CPAI-2023-1853	CVE-2023-33404	BlogEngine.NET の任意のファイルがアップロードされる脆弱性 (CVE-2023-33404)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［BlogEngine.NET Arbitrary File Upload (CVE-2023-33404)］保護機能を探し、保護機能の設定を編集します。
緊急	2024年8月5日	CPAI-2023-1859	CVE-2023-6612	TOTOLINK X5000R のコマンド インジェクション (CVE-2023-6612)	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 X5000R Command Injection (CVE-2023-6612)］保護機能を探し、保護機能の設定を編集します。