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12月4日	CPAI-2022-1003	CVE-2022-1556	WordPress StaffList プラグインの SQL インジェクション (CVE-2022-1556)	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 StaffList Plugin SQL Injection (CVE-2022-1556)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年12月6日	CPAI-2021-0894	CVE-2021-42237	Sitecore XP のリモートからコードを実行される脆弱性 (CVE-2021-42237)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Sitecore XP Remote Code Execution (CVE-2021-42237)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年12月4日	CPAI-2022-0967	CVE-2022-25445 CVE-2022-25446 CVE-2022-25447 CVE-2022-25448 CVE-2022-25449 CVE-2022-25452 CVE-2022-25453 CVE-2022-25456 CVE-2022-25458	Tenda AC6 のスタック オーバーフロー (CVE-2022-25445; CVE-2022-25446; CVE-2022-25447; CVE-2022-25448; CVE-2022-25449; CVE-2022-25452; CVE-2022-25453; CVE-2022-25456; CVE-2022-25458)	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 AC6 Stack Overflow (CVE-2022-25445)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年12月4日	CPAI-2022-1009	CVE-2022-37159	Claroline で任意のファイルがアップロードされる脆弱性 (CVE-2022-37159)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Claroline Arbitrary File Upload (CVE-2022-37159)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年12月4日	CPAI-2022-0974	CVE-2022-30472 CVE-2022-30474 CVE-2022-30476 CVE-2022-30477 CVE-2022-38309 CVE-2022-38310 CVE-2022-38311 CVE-2022-38312 CVE-2022-38313 CVE-2022-38314 CVE-2022-40854	Tenda AC18 バッファ オーバーフロー (CVE-2022-30472; CVE-2022-30474; CVE-2022-30476; CVE-2022-30477; CVE-2022-38309; CVE-2022-38310; CVE-2022-38311; CVE-2022-38312; CVE-2022-38313; CVE-2022-38314; CVE-2022-40854)	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 AC18 Buffer Overflow］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-2022-0746	CVE-2022-28895 CVE-2022-28896 CVE-2022-28901	D-Link DIR882 のコマンドインジェクション (CVE-2022-28895; CVE-2022-28896; CVE-2022-28901)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［D-Link DIR882 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12月4日	CPAI-2022-0975	CVE-2022-27984 CVE-2022-27985	CuppaCMS のSQL インジェクション (CVE-2022-27984; CVE-2022-27985)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［CuppaCMS SQL Injection］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20日	CPAI-2022-0864	CVE-2022-26206 CVE-2022-26207 CVE-2022-26208 CVE-2022-26209 CVE-2022-26210 CVE-2022-26211 CVE-2022-26212 CVE-2022-26214 CVE-2022-27003 CVE-2022-27004 CVE-2022-27005 CVE-2022-28935	TOTOLINK ルータのコマンドインジェクション (CVE-2022-26206; CVE-2022-26207; CVE-2022-26208; CVE-2022-26209; CVE-2022-26210; CVE-2022-26211; CVE-2022-26212; CVE-2022-26214; CVE-2022-27003; CVE-2022-27004; CVE-2022-27005; CVE-2022-28935)	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 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12月4日	CPAI-2022-0976	CVE-2022-28127	Robustel R1510 で任意のファイルが削除される脆弱性 (CVE-2022-28127)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Robustel R1510 Arbitrary File Deletion (CVE-2022-28127)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年12月4日	CPAI-2022-0982	CVE-2022-37055	D-Link GO-RT-AC750 のバッファ オーバーフロー (CVE-2022-37055)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［D-Link GO-RT-AC750 Buffer Overflow (CVE-2022-37055)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年12月4日	CPAI-2022-0940	CVE-2022-28373 CVE-2022-28374 CVE-2022-28375	Verizon LVSKIHP のコマンドインジェクション (CVE-2022-28373; CVE-2022-28374; CVE-2022-28375)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Verizon LVSKIHP 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12月4日	CPAI-2022-0993	CVE-2022-24218	eliteCMS で任意のファイルが削除される脆弱性 (CVE-2022-24218)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［eliteCMS Arbitrary File Deletion (CVE-2022-24218)］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28日	CPAI-2022-0946	CVE-2022-35619 CVE-2022-35620	D-Link DIR-818LW のコマンドインジェクション (CVE-2022-35619; CVE-2022-35620)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［D-Link DIR-818LW Command Injection (CVE-2022-35619; CVE-2022-35620)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年12月5日	CPAI-2021-1319	CVE-2021-25216	ISC BIND で発見された整数オーバーフロー (CVE-2021-25216)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［ISC BIND Integer Overflow (CVE-2021-25216)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年12月5日	CPAI-2022-1008	CVE-2022-38555	Linksys E1200 で発見されたバッファオーバーフロー (CVE-2022-38555)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Linksys E1200 Buffer Overflow (CVE-2022-38555)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年12月5日	CPAI-2021-1451	CVE-2021-2456	Oracle Fusion Middleware Business Intelligence の安全でないデシアライゼーション (CVE-2021-2456)	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 Fusion Middleware Business Intelligence Insecure Deserialization (CVE-2021-2456)］保護機能を探し、保護機能の設定を編集します。