

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5月8日	CPAI-2010-0669	CVE-2010-5330	Ubiquiti AirOS のコマンドインジェクションの脆弱性 (CVE-2010-5330)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Ubiquiti AirOS Command Injection (CVE-2010-5330)] 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8日	CPAI-2018-1801	CVE-2018-20753	Kaseya VSA のリモートからコードを実行される脆弱性 (CVE-2018-20753)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Kaseya VSA Remote Code Execution (CVE-2018-20753)] 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8日	CPAI-2021-1172	CVE-2021-46314 CVE-2021-46315 CVE-2021-46319	D-Link DIR-846 のコマンドインジェクションの脆弱性 (CVE-2021-46314; CVE-2021-46315; CVE-2021-46319)	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-846 Command Injection (CVE-2021-46314)] 保護機能を探し、保護機能の設定を編集します。
高	2022年5月9日	CPAI-2022-0216		Seowon SLC-130 ルータのリモートからコードを実行される脆弱性	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Seowon SLC-130 Router Remote Code Execution] 保護機能を探し、保護機能の設定を編集します。
高	2022年5月10日	CPAI-2022-0236	CVE-2022-28818 APSB22-22	Adobe ColdFusion のクロスサイトスクリプティング (APSB22-22: CVE-2022-28818)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Adobe ColdFusion Cross-site Scripting (APSB22-22: CVE-2022-28818)] 保護機能を探し、保護機能の設定を編集します。
高	2022年5月10日	CPAI-2022-0235	CVE-2022-29104	Microsoft Windows 印刷スプーラーで発見された特権が昇格される脆弱性 (CVE-2022-29104)	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 Windows Print Spooler Elevation of Privilege (CVE-2022-29104)] 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10日	CPAI-2022-0225	CVE-2022-22017	Microsoft リモート デスクトップ クライアントのリモートからコードを実行される脆弱性 (CVE-2022-22017)	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 Remote Desktop Client Remote Code Execution (CVE-2022-22017)] 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10日	CPAI-2022-0224	CVE-2022-23270	Microsoft Point-to-Point Tunneling プロトコルのリモートからコードを実行される脆弱性 (CVE-2022-23270)	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 Point-to-Point Tunneling Protocol Remote Code Execution (CVE-2022-23270)] 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10日	CPAI-2022-0223	CVE-2022-26923	Microsoft Active Directory のドメイン サービスで特権が昇格される脆弱性 (CVE-2022-26923)	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 Active Directory Domain Services Elevation of Privilege (CVE-2022-26923)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年4月3日	CPAI-2022-0107	CVE-2022-22947	Spring Cloud Gateway のリモートからコードを実行される脆弱性 (CVE-2022-22947)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Spring Cloud Gateway Remote Code Execution (CVE-2022-22947)] 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5月15日	CPAI-2021-1171	CVE-2021-23450	Dojo のプロトタイプ汚染攻撃 (CVE-2021-23450)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Dojo Prototype Pollution (CVE-2021-23450)] 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15日	CPAI-2019-2528	CVE-2019-1003029	Jenkins Script Security プラグインのリモートからコードを実行される脆弱性 (CVE-2019-1003029)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Jenkins Script Security Plugin Remote Code Execution (CVE-2019-1003029)] 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17日	CPAI-2022-0241	CVE-2022-26937	Microsoft Windows ネットワーク ファイル システムのリモートからコードを実行される脆弱性 (CVE-2022-26937)	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 Windows Network File System Remote Code Execution (CVE-2022-26937)] 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17日	CPAI-2017-1223	CVE-2017-12478	Kaseya Unitrends Backup のリモートからコードを実行される脆弱性 (CVE-2017-12478)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Kaseya Unitrends Backup Remote Code Execution (CVE-2017-12478)] 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の脆弱性 (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5月19日	CPAI-2022-0246	CVE-2022-29081	Zoho の複数製品の認証を回避される脆弱性 (CVE-2022-29081)	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 Multiple Products Authentication Bypass (CVE-2022-29081)] 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23日	CPAI-2022-0249	CVE-2022-0441	WordPress MasterStudy LMS プラグインの権限が昇格される脆弱性 (CVE-2022-0441)	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 MasterStudy LMS Plugin Privilege Escalation (CVE-2022-0441)] 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23日	CPAI-2022-0244	CVE-2022-29904	MediaWiki Semantic Drilldown の SQL インジェクション (CVE-2022-29904)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [MediaWiki Semantic Drilldown SQL Injection (CVE-2022-29904)] 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-2021-1183	CVE-2021-46441 CVE-2021-46442	D-Link DIR-825 OS のコマンドインジェクションの脆弱性 (CVE-2021-46441; CVE-2021-46442)	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-825 OS Command Injection (CVE-2021-46441)] 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 Firewall の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。