

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2月28日	CPAI-2021-1099	CVE-2021-40865	Apache Storm のリモートからコードを実行される脆弱性 (CVE-2021-40865)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Apache Storm Remote Code Execution (CVE-2021-40865)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年2月28日	CPAI-2021-1095	CVE-2021-43711	TOTOLINK EX200 のコマンドインジェクション (CVE-2021-43711)	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 EX200 Command Injection (CVE-2021-43711)] 保護機能を探し、保護機能の設定を編集します。
高	2022年3月1日	CPAI-2006-0387	CVE-2006-1547	Apache Struts のサービス拒否 (DoS) 攻撃 (CVE-2006-1547)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Apache Struts Denial of Service (CVE-2006-1547)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年3月2日	CPAI-2022-0052	CVE-2022-23131	Zabbix Web フロントエンドの認証を回避される脆弱性 (CVE-2022-23131)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Zabbix Web Frontend Authentication Bypass (CVE-2022-23131)] 保護機能を探し、保護機能の設定を編集します。
高	2022年3月7日	CPAI-2021-1096	CVE-2021-42362	WordPress Popular Posts プラグインの任意のファイルがアップロードされる脆弱性 (CVE-2021-42362)	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 Popular Posts Plugin Arbitrary File Upload (CVE-2021-42362)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年3月7日	CPAI-2020-3459	CVE-2020-7209	HP LinuxKI のコマンドインジェクション (CVE-2020-7209)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [HP LinuxKI Command Injection (CVE-2020-7209)] 保護機能を探し、保護機能の設定を編集します。
高	2022年3月8日	CPAI-2022-0068	CVE-2022-23285	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-2022-23285)	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-2022-23285)] 保護機能を探し、保護機能の設定を編集します。
高	2022年3月8日	CPAI-2022-0058	CVE-2022-23299	Microsoft Windows PDEV の権限が昇格される脆弱性 (CVE-2022-23299)	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 PDEV Elevation of Privilege (CVE-2022-23299)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年3月10日	CPAI-2021-1103	CVE-2021-44521	Apache Cassandra のリモートからコードを実行される脆弱性 (CVE-2021-44521)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Apache Cassandra Remote Code Execution (CVE-2021-44521)] 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3月10日	CPAI-2021-1070	CVE-2021-33266 CVE-2021-33267 CVE-2021-33268 CVE-2021-33269 CVE-2021-33270 CVE-2021-33271 CVE-2021-33274	D-Link DIR809 のバッファオーバーフロー (CVE-2021-33266; CVE-2021-33267; CVE-2021-33268; CVE-2021-33269; CVE-2021-33270; CVE-2021-33271; CVE-2021-33274)	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 DIR809 Buffer Overflow (CVE-2021-33266)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年3月13日	CPAI-2020-3451	CVE-2020-25765 CVE-2020-27158 CVE-2020-27159 CVE-2020-27160 CVE-2020-27744	Western Digital My Cloud NAS のリモートからコードを実行される複数の脆弱性 (CVE-2020-25765; CVE-2020-27158; CVE-2020-27159; CVE-2020-27160; CVE-2020-27744)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Western Digital My Cloud NAS Remote Code Execution Multiple Vulnerabilities] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年3月16日	CPAI-2021-1110	CVE-2021-44515	Zoho ManageEngine Desktop Central で認証が回避される脆弱性 (CVE-2021-44515)	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 Desktop Central Authentication Bypass (CVE-2021-44515)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年3月27日	CPAI-2022-0094	CVE-2022-0609	Google Chrome の解放後メモリ利用の脆弱性 (CVE-2022-0609)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Google Chrome Use After Free (CVE-2022-0609)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年3月28日	CPAI-2021-1025	CVE-2021-36260	Hikvision Web Server のコマンドインジェクション (CVE-2021-36260)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Hikvision Web Server Command Injection (CVE-2021-36260)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年3月29日	CPAI-2022-0084	CVE-2022-24086	Adobe Commerce のコマンドインジェクション (CVE-2022-24086)	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 Commerce Command Injection (CVE-2022-24086)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年3月30日	CPAI-2021-1116	CVE-2021-37973	Google Chrome ブラウザの解放後メモリ利用の脆弱性 (CVE-2021-37973)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Google Chrome Browser Use-After-Free (CVE-2021-37973)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年3月30日	CPAI-2021-1148	CVE-2021-46393 CVE-2021-46394	Tenda AX3 ルータのバッファオーバーフロー (CVE-2021-46393; CVE-2021-46394)	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 Buffer Overflow (CVE-2021-46393; CVE-2021-46394)] 保護機能を探し、保護機能の設定を編集します。
緊急	2022年3月30日	CPAI-2021-1072	CVE-2021-44352	Tenda AC15 のバッファオーバーフロー (CVE-2021-44352)	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 AC15 Buffer Overflow (CVE-2021-44352)] 保護機能を探し、保護機能の設定を編集します。