

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	2023年2月14日	CPAI-2023-0073	CVE-2023-21689	Microsoft PEAP (Protected Extensible Authentication Protocol) のリモートからコードを実行される脆弱性 (CVE-2023-21689)	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 Protected Extensible Authentication Protocol Remote Code Execution (CVE-2023-21689)] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年2月14日	CPAI-2023-0074	CVE-2023-21692	Microsoft PEAP (Protected Extensible Authentication Protocol) のリモートからコードを実行される脆弱性 (CVE-2023-21692)	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 Protected Extensible Authentication Protocol Remote Code Execution (CVE-2023-21692)] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年2月14日	CPAI-2023-0075	CVE-2023-21690	Microsoft PEAP (Protected Extensible Authentication Protocol) のリモートからコードを実行される脆弱性 (CVE-2023-21690)	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 Protected Extensible Authentication Protocol Remote Code Execution (CVE-2023-21690)] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年2月15日	CPAI-2022-1162	CVE-2022-4873	Netcomm のバッファオーバーフロー (CVE-2022-4873)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Netcomm Buffer Overflow (CVE-2022-4873)] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年2月15日	CPAI-2022-1163	CVE-2022-4606	FlatPress で任意のファイルがアップロードされる脆弱性 (CVE-2022-4606)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [FlatPress Arbitrary File Upload (CVE-2022-4606)] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年2月15日	CPAI-2018-2316	CVE-2018-17254	Joomla! JCK Editor コンポーネントの SQL インジェクション (CVE-2018-17254)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Joomla! JCK Editor Component SQL Injection (CVE-2018-17254)] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年2月16日	CPAI-2022-1159	CVE-2022-4101	WordPress Images Optimize and Upload CF7 プラグインのディレクトリトラバーサル (CVE-2022-4101)	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 Images Optimize and Upload CF7 Plugin Directory Traversal (CVE-2022-4101)] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年2月19日	CPAI-2023-0072	CVE-2023-0245 CVE-2023-0283	Online Flight Booking Management System の SQL インジェクション (CVE-2023-0245; CVE-2023-0283)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Online Flight Booking Management System SQL Injection] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年2月19日	CPAI-2022-1221	CVE-2022-46476	D-Link DIR-859 のコマンドインジェクション (CVE-2022-46476)	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-859 Command Injection (CVE-2022-46476)] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年2月19日	CPAI-2022-1222	CVE-2022-46475	D-Link DIR 645A1 のスタックオーバーフロー (CVE-2022-46475)	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 645A1 Stack Overflow (CVE-2022-46475)] 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	2023年2月20日	CPAI-2021-1618	CVE-2021-21243	OneDev で認証をバイパスされる脆弱性 (CVE-2021-21243)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [OneDev Authentication Bypass (CVE-2021-21243)] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年2月21日	CPAI-2022-1216	CVE-2022-4855	Lead Management System の SQL インジェクション (CVE-2022-4855)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Lead Management System SQL Injection (CVE-2022-4855)] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年2月21日	CPAI-2020-3734	CVE-2020-35326	inxedu の SQL インジェクション (CVE-2020-35326)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [inxedu SQL Injection (CVE-2020-35326)] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年2月22日	CPAI-2020-3423	CVE-2020-25223	Sophos SG UTM のコマンドインジェクション (CVE-2020-25223)	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 SG UTM Command Injection (CVE-2020-25223)] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年2月23日	CPAI-2022-1233	CVE-2022-24697	Apache Kylin のコマンドインジェクション (CVE-2022-24697)	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 Kylin Command Injection (CVE-2022-24697)] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年2月26日	CPAI-2022-1236	CVE-2022-4120	WordPress Stop Spammers Security プラグインの安全でないデシリアライゼーション (CVE-2022-4120)	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 Stop Spammers Security Plugin Insecure Deserialization (CVE-2022-4120)] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年2月9日	CPAI-2022-1181	CVE-2022-45709 CVE-2022-45711 CVE-2022-45717	IP-COM M50 のコマンドインジェクション (CVE-2022-45709; CVE-2022-45711; CVE-2022-45717)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [IP-COM M50 Command Injection] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年3月2日	CPAI-2023-0103	CVE-2023-23076	Zoho ManageEngine SupportCenter Plus のコマンドインジェクション (CVE-2023-23076)	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 SupportCenter Plus Command Injection (CVE-2023-23076)] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年3月7日	CPAI-2022-1323	CVE-2022-46887	NexusPHP の SQL インジェクション (CVE-2022-46887)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [NexusPHP SQL Injection (CVE-2022-46887)] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年3月8日	CPAI-2021-1676	CVE-2021-43267	Linux Kernel TIPC ヒープオーバーフロー (CVE-2021-43267)	SmartDashboard の [IPS] タブを選択し、[Protections] を選択します。検索機能を使って [Linux Kernel TIPC Heap Overflow (CVE-2021-43267)] 保護機能を探し、保護機能の設定を編集します。
緊急	2023年3月8日	CPAI-2022-1326	CVE-2022-3900	WordPress Cooked Pro プラグインの安全でないデシリアライゼーション (CVE-2022-3900)	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 Cooked Pro Plugin Insecure Deserialization (CVE-2022-3900)] 保護機能を探し、保護機能の設定を編集します。