Software Vulnerability Research Release Notes

September 2020

Introduction

Software Vulnerability Research provides access to verified intelligence from Secunia Research, covering all applications and systems across all platforms. Prioritization is driven by threat intelligence, workflows, tickets and alerts, and describes the steps to mitigate the risk of costly breaches. You stay in control and hackers stay out. For more information, see https://www.flexera.com/products/operations/software-vulnerability-research.html

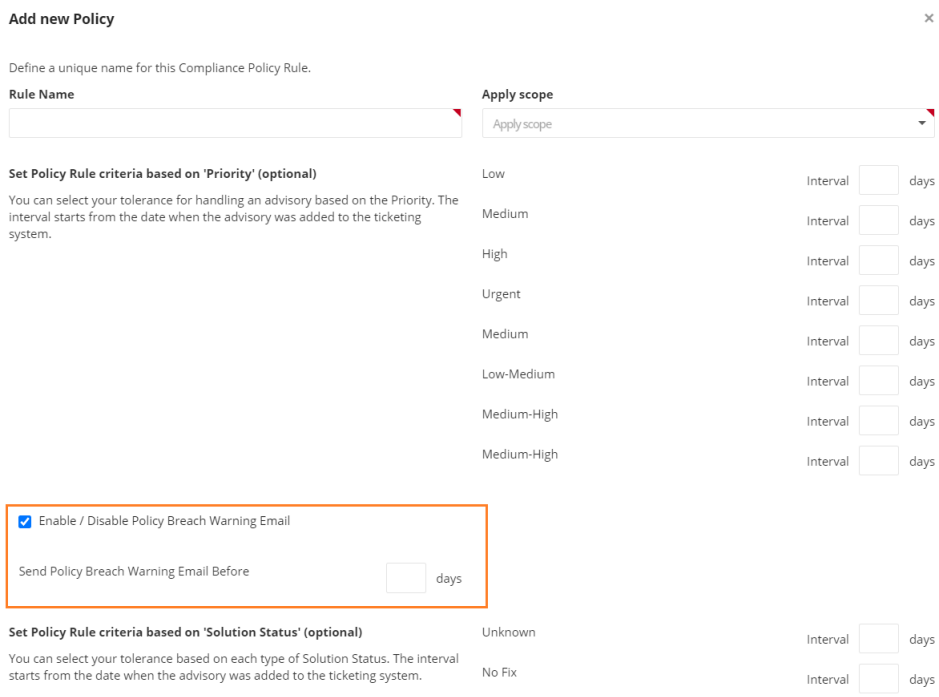
New Features and Enhancements

This Software Vulnerability Research update includes the following:

- Email Warning before Policy Breach
- Renamed Whitelist / Blacklist to Allow List / Block List
- API User Management Role Access to the User Data
- Enforced Special Characters for the Password

Email Warning before Policy Breach

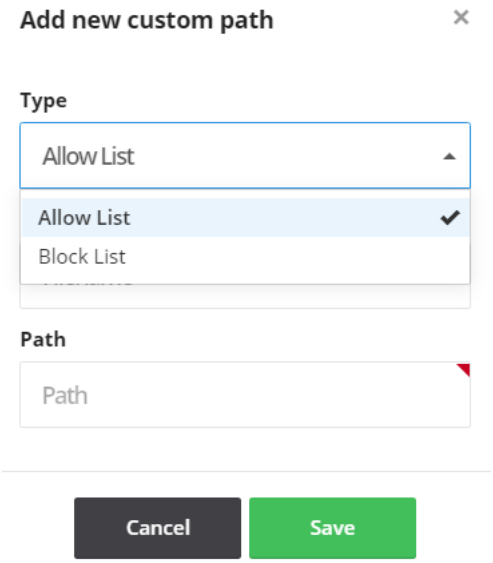
With this new feature, you will be able to send a policy breach warning emails for applicable open or waiting tickets. This warning can be configured for priority based rule of the policy and will enable the ticket assignees to prioritize their tickets. You will be able to configure the number of days before the policy breach, to send such a warning.



For more details, see Policies.

Renamed Whitelist / Blacklist to Allow List / Block List

With this update, terms Whitelist / Blacklist has been renamed to **Allow List** / **Block List** respectively.



For more details, see Add Custom Scan Paths

API User Management Role Access to the User Data

With this update, users with API User Management Role will now be able to access the user data using the API - `https://api.app.flexerasoftware.com/api/users/`

Enforced Special Characters for the Password

With this update, passwords will require at least one special character. This will apply to new user setup, password reset, and forgot passwords.

System Requirements

Software Vulnerability Research's user interface will resize and adapt when being used on different devices. You can access the system from anywhere using any device, such as a smart phone or tablet, running Internet Explorer 11 or higher, Chrome, Opera, Firefox, Safari and mobile browsers with an Internet connection capable of connecting to https://app.flexerasoftware.com.

Resolved Issues

The following table lists the customer issues that were resolved in Software Vulnerability Research :

Issue	Description
IOJ-02203019	Enforced SSO login for non-root user if standard login disabled. A bug that allowed the user with multiple roles to use standard login even though it disabled for SSO is fixed.

Legal Information

Copyright Notice

Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see https://www.flexera.com/legal/intellectual-property.html. All other brand and product names mentioned in Flexera products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.