SecPoint® Penetrator Vulnerability Scanner V 70

Firmware Release

https://www.SecPoint.com/penetrator.html

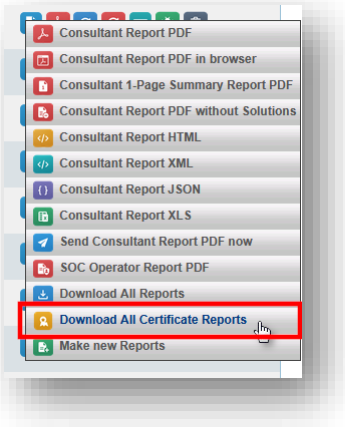




Penetrator 70 – October 2026

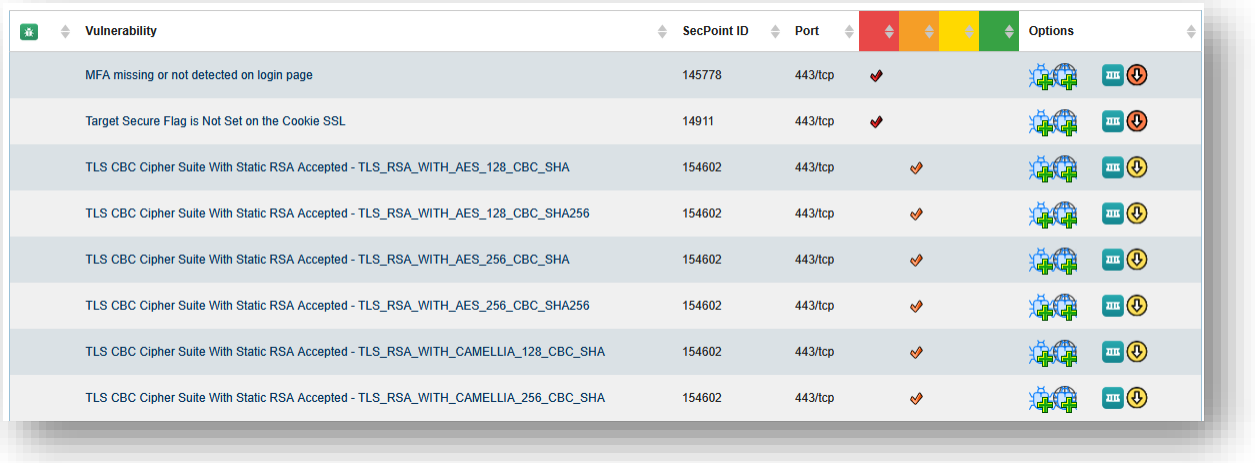
- **Download All Certificate Reports**

Firmware 70 adds a convenient way to download the Certificate reports for every target in a scan in one archive. From the scan list on the Home page, open the scan's floating menu and select *Download All Certificate Reports*.
Penetrator checks the scan and its access permissions, then processes the scan's targets one by one. A Certificate is generated when needed and added to a ZIP file. The archive contains Certificate reports only, so it can be stored or shared separately from the scan's other reports.
The existing action *Download All Reports* will also download the available target Certificates.



- **More Robust Vulnerability Output Parsing**

The vulnerability output parser has additional checks to handle malformed records before they reach the database.
Parsing is part of scan processing: after the scanner output is analyzed, Penetrator extracts vulnerability details and stores the results for later display and reporting.



Vulnerability	SecPoint ID	Port					Options
MFA missing or not detected on login page	145778	443/tcp	✓				
Target Secure Flag is Not Set on the Cookie SSL	14911	443/tcp	✓				
TLS CBC Cipher Suite With Static RSA Accepted - TLS_RSA_WITH_AES_128_CBC_SHA	154602	443/tcp		✓			
TLS CBC Cipher Suite With Static RSA Accepted - TLS_RSA_WITH_AES_128_CBC_SHA256	154602	443/tcp		✓			
TLS CBC Cipher Suite With Static RSA Accepted - TLS_RSA_WITH_AES_256_CBC_SHA	154602	443/tcp		✓			
TLS CBC Cipher Suite With Static RSA Accepted - TLS_RSA_WITH_AES_256_CBC_SHA256	154602	443/tcp		✓			
TLS CBC Cipher Suite With Static RSA Accepted - TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	154602	443/tcp		✓			
TLS CBC Cipher Suite With Static RSA Accepted - TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	154602	443/tcp		✓			

The parser validates required fields and accepted risk values, checks numeric SPID values, and rejects duplicate single-value fields. It also limits the size of an individual vulnerability

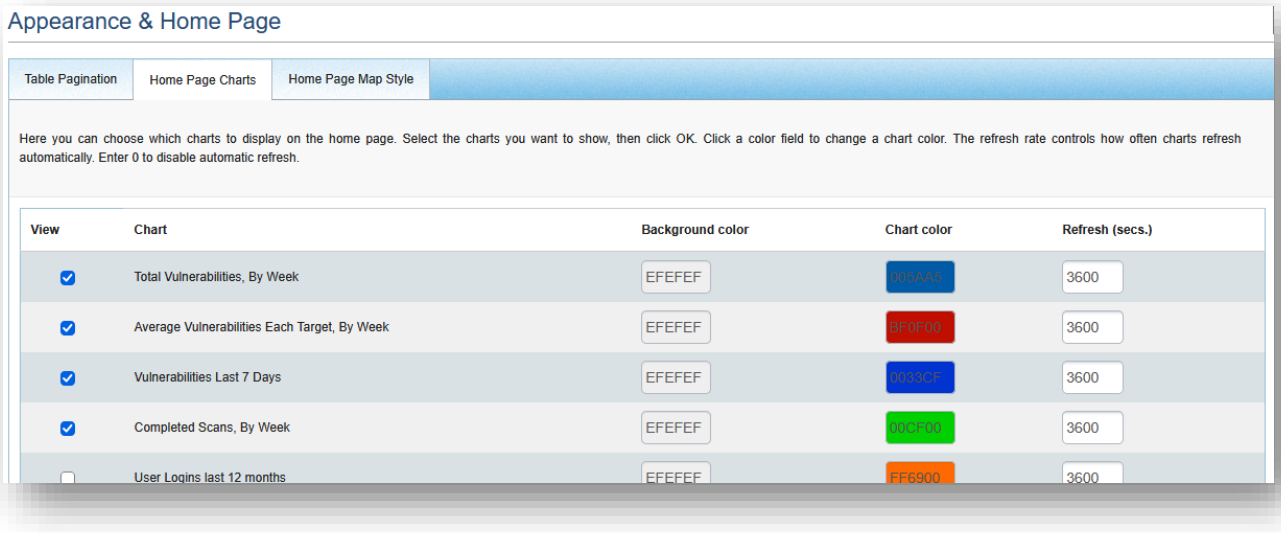
record. Invalid records are skipped and recorded as concise diagnostics during result storage, helping prevent malformed scanner output from causing database errors.

This is an automatic improvement to scan processing that guarantees that the information displayed about detected vulnerabilities is always correct.

• Web interface updates

To improve visual layout and user experience, the following web interface updates have been implemented:

- New icons on the home page and floating menus: the redesigned icons offer better visual recognition and streamline menu interaction.
- Reorganized Branding Settings: The Report and Interface Branding pages have been merged into two separate tabs on a single page. You can access this new page via menu *System > Branding*.
- New *System > Appearance & Home Page* menu Settings: Table Pagination, Home Page Charts, and Home Page Map Style options are now grouped under this new page.



• Security Updates for PHP and Web Sessions

Security has received particular attention in Firmware 70. The appliance installs PHP 8.4.27, a security release that addresses two recently disclosed critical vulnerabilities.

Keeping the PHP runtime current helps protect the appliance against known weaknesses in the underlying platform.

The web application also uses the *HttpOnly* and *SameSite* cookie attributes. These browser-enforced protections help reduce the risk of session cookies being exposed to scripts or sent in unwanted cross-site requests.



In addition, PHP session upload-progress tracking is now disabled. Together, these measures reinforce the protection of login sessions while remaining transparent during normal use.

- **And…**

  - Watermark "Confidential" set by default for reports on factory reset
  - Metasploit installation without SQL
  - Reorganization of System menu in a better and more intuitive way
  - Direct link to the function that compares 2 scans
  - Compatibility checks between MFA and Bitwarden password manager
  - Optimization of disk usage for wordlist update
  - On the Penetrator location map, a link to the map setup page has been added for admin users
  - Improved online check for Default Gateway
  - Icons replacement
  - Stronger checks to avoid blind SQL vulnerabilities
  - New background image for the login page
  - Better management of failed CSRF check when a security token has expired
  - Enhanced SMB/NetBIOS scanning across SMB1, SMB2 and SMB3, covering weak credentials, guest access, exposed or writable shares, signing weaknesses & legacy protocol risks.
  - Dark Web Search 6.3

HAFS
Distributeur à valeur ajoutée

VOTRE PARTENAIRE TECHNOLOGIQUE
POUR DES INFRASTRUCTURES IT SÉCURISÉES ET PERFORMANTES

EXPERTISE
Des solutions adaptées à chaque environnement

CONFIANCE
Un partenaire fiable à vos côtés

PERFORMANCE
Des infrastructures sécurisées et évolutives

SUPPORT
Un accompagnement technique de qualité

HAFS
Distributeur à valeur ajoutée

Des solutions IT innovantes pour un monde connecté et sécurisé

WIRELESS RADIO
Connectivité sans fil haute performance

RÉSEAUX & SÉCURITÉ IT
Des réseaux fiables et sécurisés

VIRTUALISATION CLOUD
Des solutions Cloud flexibles et évolutives

CYBERSECURITY
Protéger vos données et vos systèmes

VIDÉO PROTECTION
Solutions de vidéosurveillance intelligentes

HCI STOCKAGE SAUVEGARDE
Stockage, sauvegarde et haute disponibilité

SOLUTIONS IT | CYBERSÉCURITÉ | CLOUD | INFRASTRUCTURE RÉSEAU | STOCKAGE | PROTECTION



Département Commercial

HAFS
Distributeur à valeur ajoutée

Vous accompagne

HAFS NETWORKS WCA
+225 07 89 82 56 49 / +225 07 59 05 85 82
sales-ci@hafs-networks.com

HAFS NETWORKS FRANCE
+33 (0)7 49 92 62 57 / +33(0)9 73 89 20 39
sales@hafs-networks.com

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

Hillstone NETWORKS | Synology | SANGFOR | SECPOINT | Axidian | NEOWAVE | HORNETSECURITY FORMERLY vade | CyberShield

RUCKUS NETWORKS | Ruijie Reyee | RAY | Wiflyx | SEARCHINFORM | MOBOTIX | EXTRAVIS | HAFS MediVision