Web Security On-prem and URL Filtering

8.5.7

Release Notes

Revision A

Contents

Introduction

Forcepoint Web Security On-Premises and URL Filtering deliver advanced, real-time web protection with granular policy control and flexible deployment, ideal for organizations with strict data and compliance requirements.

This document summarizes the updates introduced in the Forcepoint Web Security On-Premises and URL Filtering v8.5.7 release, including new features, resolved issues, security updates, platform support enhancements, and known issues. It serves as a comprehensive guide to help you plan upgrades, maintain compliance, and stay informed about product improvements.

Note

The Content Gateway component is not included in Forcepoint URL Filtering deployments. Content Gateway information applies only to Forcepoint Web Security.

Note

Direct upgrade from 8.5.4 to 8.5.7 for DLP customer is not supported. To upgrade successfully from 8.5.4 to 8.5.7, first upgrade to DLP version included in 8.5.5 unified installer and then login to Forcepoint Security Manager (FSM) to switch to DATA and allow the policies to be updated. After that upgrade to 8.5.7.

Customers using Red Hat Enterprise Linux versions earlier than 8.10 must upgrade their operating system before installing this product release.

New features

Enhanced security with TLS 1.3 support

TLS 1.3 support is now fully integrated into the codebase, enhancing secure communications across the product.

The product exclusively uses strong cipher suites recommended by the product security team, aligning with industry cryptographic best practices to improve security posture.

This update helps to protect against vulnerabilities found in older ciphers while ensuring compatibility with modern security standards.

Expanded platform support for Enterprise Linux

Platform compatibility has been extended to include Red Hat Enterprise Linux 8 and Oracle Linux 8.

This update enables organizations to deploy the product on modern enterprise-grade Linux environments, enhancing stability, performance, and long-term support while aligning with current operating system lifecycle policies.

Security updates

Security updates are implemented based on comprehensive inputs from Forcepoint Security Labs, third-party library maintainers, internal research, and customer vulnerability reports to effectively address potential security risks.

Version 8.5.7 includes the following security updates

Updates	Description	CVE	CWE
SSL/TLS renegotiation Denial of Service (DoS) vulnerability.	SSL/TLS renegotiation requests were not restricted, allowing attackers to exploit the handshake process and exhaust server resources. This issue is fixed through configuration changes that limit renegotiation and enable secure cryptographic negotiation.	CVE-2009-3555	CWE-295

Updates	Description	CVE	CWE
Stored XSS vulnerability on blockpage/ blockOptions.cgi.	A stored cross-site scripting (XSS) vulnerability was identified in the `/cgi-bin/blockOptions.cgi` and `/cgi-bin/blockpage.cgi` endpoints, allowing an attacker to inject malicious scripts. This issue is fixed with user input sanitization to prevent script execution.	CVE-2025-2274	CWE-79
Multiple vulnerabilities in Apache Tomcat versions 9.0.76 through 9.0.102.	Apache Tomcat needs to be upgraded to version 9.0.104 to fix multiple vulnerabilities, including time-of-check to time-of-use (TOCTOU) race conditions, resource exhaustion, and authentication issues.	■ CVE-2024-34750 ■ CVE-2024-38286 ■ CVE-2024-50379 ■ CVE-2024-52316 ■ CVE-2024-54677 ■ CVE-2024-56337 ■ CVE-2025-31650	■ CWE-367 ■ CWE-391 ■ CWE-400 ■ CWE-770
Multiple vulnerabilities in Apache 2.4.x versions prior to 2.4.60.	Multiple vulnerabilities were identified in Apache HTTP Server versions earlier than 2.4.60, including null pointer dereference, SSRF, and improper handling of URLs and encoding issues. This issue is fixed with an upgrade to version 2.4.60.	■ CVE-2024-36387 ■ CVE-2024-38472 ■ CVE-2024-38473 ■ CVE-2024-38474 ■ CVE-2024-38475 ■ CVE-2024-38477 ■ CVE-2024-39573	■ CWE-116 ■ CWE-20 ■ CWE-476 ■ CWE-918
Multiple vulnerabilities in OpenJDK 8 up to version 8u422.	Multiple vulnerabilities in OpenJDK 8 up to version 8u422 allow attackers to gain unauthorized access to modify or delete critical data. This issue is fixed with an upgrade to the latest available version.	■ CVE-2024-20918 ■ CVE-2024-20919 ■ CVE-2024-20921 ■ CVE-2024-20926 ■ CVE-2024-20932 ■ CVE-2024-20945 ■ CVE-2024-20952	■ CWE-276 ■ CWE-284 ■ NVD-CWE-noinfo
Heap buffer overflow in libcurl versions 7.69 to earlier than 8.4.0.	The libcurl version on the remote host has a heap buffer overflow in the SOCKS5 proxy handshake, which attackers could exploit to crash the system or execute code. This issue is fixed with an upgrade to libcurl 8.4.0 or later.	CVE-2023-38545	CWE-787

Updates	Description	CVE	CWE
Apache ZooKeeper upgrade to 3.8.4.	Apache ZooKeeper 3.4.14 has vulnerabilities that allow attackers to monitor znode paths without permission and enable unauthorized users to join the cluster due to an authentication flaw. This issue is fixed with an upgrade to version 3.8.4.	■ CVE-2024-23944 ■ CVE-2023-44981	■ CWE-200 ■ CWE-639
Eclipse Jetty DoS vulnerability.	Vulnerabilities in Eclipse Jetty versions 9.4.6.v20170531 to 9.4.36.v20210114, 10.0.0, and 11.0.0 cause high CPU usage and DoS when processing requests with multiple accept headers containing many quality (q) parameters. This issue is fixed with an upgrade to the latest version.	■ CVE-2020-27216 ■ CVE-2020-27218 ■ CVE-2020-27223 ■ CVE-2021-28165 ■ CVE-2021-28169 ■ CVE-2021-3328 ■ CVE-2021-34428	■ CWE-125 ■ CWE-200 ■ CWE-226 ■ CWE-378 ■ CWE-400 ■ CWE-407 ■ CWE-613 ■ CWE-755
Outdated SSL/TLS protocols and Ciphers on port 15873.	The Web Management API on port 15873 in SWG 8.5.5 and earlier allowed insecure SSL/TLS protocols and cipher suites. This issue is fixed by disabling deprecated protocols and aligning with secure configuration guidelines.	■ CVE-2013-2566 ■ CVE-2014-3566 ■ CVE-2015-2808 ■ CVE-2016-2183 ■ CVE-2016-6329	■ CWE-200 ■ CWE-310 ■ CWE-326 ■ CWE-327
Multiple vulnerabilities in Apache HTTP Server versions prior to 2.4.59.	Apache HTTP Server versions through 2.4.58 contain input validation flaws and response handling vulnerabilities that could lead to HTTP response splitting and memory exhaustion. This issue is fixed with an upgrade to the latest available version.	■ CVE-2023-38709 ■ CVE-2024-24795 ■ CVE-2024-27316	■ CWE-400 ■ CWE-770
Cookie injection vulnerability in libcurl versions 7.9.1 to earlier than 8.4.0.	A cookie injection vulnerability in libcurl allows a malicious server to set arbitrary cookies for arbitrary domains. This issue is fixed with an upgrade to the latest available version.	CVE-2023-38546	None

Updates	Description	CVE	CWE
Multiple vulnerabilities in Apache HTTP Server versions prior to 2.4.62.	Apache HTTP Server versions earlier than 2.4.62 are affected by multiple vulnerabilities, including improper content handling and Server-Side Request Forgery (SSRF) risks. These issues are fixed with an upgrade to Apache version 2.4.62.	■ CVE-2024-40725 ■ CVE-2024-40898 ■ CVE-2024-39884	■ CWE-668 ■ CWE-918
Boolean-based SQL injection in Forcepoint web portal.	The Forcepoint web portal's report generator is vulnerable to a Boolean-based blind SQL injection through the "sortColumnName" and "direction" parameters. This issue is fixed with an update to address the SQL injection vulnerability.	CVE-2023-6453	None
Transition to TLS cipher suites recommended by product security team.	TLS 1.3 support has been added starting with version 8.5.7 to align with platform support. This update also adopts the strong cipher suites recommended in the Cryptographic best practices.	None	None
Missing HTTP security headers in RAPWEB interface.	The RAPWEB interface (web-based admin portal) in Forcepoint Security Manager 8.5.4 SK11 was missing key HTTP security headers on ports 55835 and 55836. This issue is fixed by adding the required headers to enhance web application security.	■ CVE-2003-1567 ■ CVE-2004-2320 ■ CVE-2010-0386	■ CWE-16 ■ CWE-200
Password disclosure in SWG log database connection.	A flaw in the Log Server's "Test Connection" feature allowed credentials to be sent in plain text to a remote host when reconfigured. This issue is fixed by improving the authentication mechanism to prevent credential exposure.	None	None

Updates	Description	CVE	CWE
Eclipse Jetty DoS vulnerability.	Multiple vulnerabilities in Eclipse Jetty could allow attackers to cause denial of service or leak sensitive information through malformed requests, improper parsing, and inadequate input validation. These issues are fixed with an upgrade to the latest available version.	CVE-2021-28165 CVE-2022-2047 CVE-2022-2048 CVE-2023-26048 CVE-2023-26049 CVE-2023-36479 CVE-2023-40167	CWE-130 CWE-149 CWE-20 CWE-200 CWE-400 CWE-410 CWE-755 CWE-770 NVD-CWE-Other NVD-CWE-noinfo
Heap read overflow in libcurl versions 7.32.0 to earlier than 8.9.1.	A flaw in libcurl's ASN1 parser could lead to a heap read overflow when processing malformed Generalized Time fields, potentially causing a crash or exposing sensitive memory contents. This issue is fixed in version 8.9.1 through a corrected parser implementation that replaces an earlier incomplete fix.	CVE-2024-7264	CWE-125
Spring Security authorization bypass vulnerability.	In Spring Security versions 5.5.6, 5.6.3, and older unsupported versions, `RegexRequestMatcher` could be misconfigured in a way that allows authorization bypass on certain servlet containers. Regular expressions containing `.` were especially prone to being bypassed. The issue is fixed with an upgrade to Spring Security version 5.7.14.	CVE-2022-22978	CWE-863
Multiple Spring Framework vulnerabilities.	Multiple vulnerabilities were identified in Spring Framework versions 3.x and 4.x. These vulnerabilities are fixed with an upgrade to Spring Framework version 5.3.39.	CVE-2024-22262 CVE-2024-38808	CWE-918 CWE-601 CWE-770

Updates	Description	CVE	CWE
Apache Commons Collections Remote Code Execution vulnerability.	A vulnerability in Apache Commons Collections prior to version 3.2.2 allowed remote code execution during object deserialization. This issue is fixed with an upgrade to Commons Collections version 3.2.2.	CVE-2015-7501	CWE-502
c3p0 XXE vulnerability in FSM Web Module.	The FSM web module was vulnerable due to the use of c3p0 version 0.9.5.2 and earlier, which allowed XML External Entity (XXE) attacks during configuration parsing. This issue is fixed by removing the dependency on c3p0.	CVE-2018-20433	CWE-611

For the basic hardware and software requirements for your system to use this product, see System requirements for this version in the Deployment and Installation Center.

Enhancements

Improvements have been made for the Hybrid Module of the Forcepoint Web Security.

Enhancement	Description
DLP Policy Engine upgrade.	Upgraded DLP Policy Engine to version 10.3 to support Oracle Linux 8.
CA tree upgrade.	Upgraded CA tree to include the latest certificate authorities for the SWG 8.5.7 release.
Proxy component platform upgrade.	Upgraded proxy components to support Oracle Linux 8, replacing deprecated Red Hat Enterprise Linux/ CentOS Linux 7.
Web Security Engine (WSE) components platform upgrade.	Upgraded WSE components to support Oracle Linux 8, replacing deprecated Red Hat Enterprise Linux/ CentOS Linux 7.
Web Content Gateway (WCG) UI update to support TLSv1.3.	Added support in the WCG UI to enable or disable TLSv1.3 under **Configure** > **SSL** > **Decryption/ Encryption**, consistent with earlier TLS version controls.
WCG UI update to support custom TLS ciphersuite configuration.	Updated the WCG UI to support user defined TLS 1.2 and TLS 1.3 ciphersuite strings via OpenSSL compliant text boxes and removed SSLv3 configuration support.

Enhancement	Description
WCG TLS ciphersuite update for custom selection.	Updated WCG to support freeform selection of TLS 1.2 and TLS 1.3 ciphersuites when set to **Custom**, updated records.config accordingly, and removed deprecated SSLv3 and TLS 1.1 support.
CCA upgrade to use Oracle Linux 8 RPM.	Updated WCG to use the Oracle Linux 8 CCA RPM from Artifactory instead of the CentOS 7 version and removed CCA code from the SWG repository.
Support for SQL Always On.	Added support for SQL Always On in the SWG 8.5.7 release.
SWG OpenSSL upgrade.	Upgraded SWG OpenSSL to version 3.0 to support TLS 1.3, replacing version 1.1.1.
HTTP cache configuration removal from SNMP.	Removed HTTP cache-related configuration settings that are safe to delete from the SNMP configuration.
HTTP cache feature removal.	Removed the HTTP cache feature from WCG as it relies on outdated technology and is ineffective with modern encrypted internet traffic.
HTTP cache monitoring removal.	Removed the cache monitoring page from the WCG UI **Monitor** tab following the removal of the HTTP cache feature.
HTTP cache configuration removal from WCG UI.	Removed the cache configuration pages for pinning, partition, and hosting from WCG UI, while keeping RAM cache size and maximum object size configurable on the **General** page.
HTTP cache monitoring removal from WCG UI Configure tab.	Removed the **HTTP Scheduled Updates** pages and section from the WCG UI **Configure** tab following the removal of the HTTP cache feature.
HTTP cache performance monitoring removal from WCG UI.	Removed all HTTP cache performance charts from the **Monitor** > **Performance** sections in WCG UI.

System requirements

To use this product, your system must meet the basic hardware and software requirements, see System requirements for this version in the Deployment and Installation Center guide.

Note

The EIP 10.2 installer requires both 32 and 64 bit Microsoft Visual C++ Redistributable packages to be installed.

Browser support

See the Certified Product Matrix for the latest list of supported browsers.

Third-party platform and product support

All components

This version supports for:

- Microsoft Windows Server 2022
- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Oracle Linux 8 and Red Hat Enterprise Linux 8.10
- VMware ESXi 8.0

This version ends support for:

- Microsoft Windows Server 2016 (all versions)
- Red Hat Enterprise Linux 7.9 and the corresponding version of CentOS

See the full list of supported operating systems here.

See the Certified Product Matrix for the latest list of supported browsers.

Content Gateway

This version is supported on:

Oracle Linux 8 and Red Hat Enterprise Linux 8.10.

Important

Forcepoint Web Security customers using Red Hat Enterprise Linux or CentOS 7.x must disable firewalld prior to installing Content Gateway.

On the machine where Content Gateway will be installed, execute the following:

```
systemctl stop firewalld
systemctl disable firewalld
```

As a best practice, Red Hat Enterprise Linux systems that host Content Gateway should be registered with Red Hat Network and kept up-to-date with the latest security patches.

Important

You can update packages on your Red Hat Enterprise Linux installations and patch kernels if the underlying kernel upgrade does not change the kernel API.

Important

Content Gateway is designed to run on a dedicated machine and is not guaranteed to be compatible with other server applications installed on the same machine.

For a complete platform requirements information, see System requirements for this version in the Deployment and Installation Center.

Resolved and known issues

Resolved issues

- Content Gateway (Forcepoint Web Security only)
- Hybrid
- Reporting and Security Information and Event Management (SIEM)

The following issues have been resolved in this v8.5.7 release:

Content Gateway (Forcepoint Web Security only)

Issue Number	Description
WSM-20293	After upgrading to WCG 8.5.6, Single Sign-On (SSO) login redirects to the WCG login page with the message `You have logged out`. This happens every time after the upgrade.

Hybrid

Issue Number	Description
WSM-20851	DC Agent service crashed due to null pointer access in the event handler logic.

Reporting and SIEM

Issue Number	Description
WSM-21428	Fixed multiple Spring Framework vulnerabilities.
WSM-19122	Spring security versions earlier than 5.5.7 and 5.6.x versions earlier than 5.6.4 were vulnerable to an authorization bypass (CVE-2022-22978).

Known issues

The current list of known issue is as follows:

Issue Number	Description	Workaround
WSM-21474	In 8.5.7, running `curl` commands after exporting the WSG library path (for example, using `LD_LIBRARY_PATH`) may result in errors due to a conflict between the version of `curl` used by the system and the version of `libcurl` used by WSG.	Run `curl` commands in a clean shell session without the custom library path, or unset `LD_LIBRARY_PATH` before using `curl`.
WSM-21472	In 8.5.7, when changing the Policy Broker mode to replica, the message `"Possible unsupported PostgreSQL version (140500) 14.5, defaulting to support for latest"` appears in the PgSetup output, even though the switch completes successfully.	This message is harmless and can be ignored. PostgreSQL 14.5 is supported. No further action is needed.
WSM-21765	On Oracle Linux 8, after proxy installation, WCG service does not start immediately after system reboot. It starts after 5 minutes, and the crontab entry for Multi Router Traffic Grapher (MRTG) is missing. The issue occurs due to incorrect permissions on `/etc/rc.d/init.d/WCG`.	Update the permissions of `/etc/rc.d/init.d/WCG` to ensure proper service startup and MRTG crontab creation.
WSM-21583	On Windows, after upgrading using Unified_Installer, services may not start automatically post-reboot. An error message is shown at the end of the upgrade process, and several services including Control Service may remain stopped.	Start the affected services manually using the WebsenseAdmin utility or Windows services.

Find product documentation

In the Forcepoint Customer Hub, you can find information about a released product, including product documentation, technical articles, and more.

You can get additional information in the Forcepoint customer hub and support for your product in the Contact Support page. In Customer hub, you can access product documentation, release notes, knowledge base articles, downloads, cases, and contact information.

You might need to log on to access the Forcepoint Customer Hub. If you do not yet have credentials, create a customer account.

Published 27 June 2025