



# ArcSight SmartConnectors

Software Version: 8.4.x

## Release Notes for Context - GeoLocation & Vulnerability Signature Updates 2024

Document Release Date: 2024

Software Release Date: 2024

## Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

## Copyright Notice

Copyright 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

## Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

## Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support-and-services/documentation>

# Release Notes for ArcSight Context - GeoLocation & Vulnerability Signature Updates 2024

This guide provides information for all the monthly Release Updates for **ArcSight Context - GeoLocation & Vulnerability Signature for the year 2024**.

Context Update which is also known as ArcSight Context - GeoLocation & Vulnerability Signature updates is delivered through ESM and Logger SKUs. Context updates are based on the following 3 factors which changes in every release:

- **Vulnerability Signatures:** Every single ArcSight release provides additional context as part of the event enrichment process and lets ESM leverage this data as it analyzes the barrage of IDS and other security alerts available for popular products like Snort, Juniper, TippingPoint, etc.
- **Sensor Signatures:** The term signature refers to signatures, rules, and filters. Customers use IPS systems to monitor networks for suspicious traffic. Mostly a set of filters or rules, which is commonly known as signatures, is designed to identify various types of network events. Signatures are often associated with vulnerabilities. ArcSight collects this information and stores it in the categorization database. Vulnerabilities are mapped to a signature. From a signature, one can find the associated vulnerabilities.
- **ipdataV6:** We have a redistribution license for Maxmind DB, which is a third-party geolocation database that is updated every week. The MaxMind and the geolocation information are distributed via a binary data file known as `ipdataV6.mmdb`.



**Important:** Every information submitted to MaxMind is subjected to modifications as they have the final destination to introduce the modifications on DB's that they provide to build the Context Builds. Every correction is reviewed by MaxMind to ensure that is accurate and complies with their policies which might take 2-3 weeks. No requests are accepted for changing anonymous proxy or VPN IP addresses.

For instructions about installing the Context updates on ESM and Logger, see [Installation Guides for Content and Context Updates](#).

## Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

## Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

## Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to [MFI-Documentation-Feedback@opentext.com](mailto:MFI-Documentation-Feedback@opentext.com).

For specific product issues, [contact Open Text Support for Micro Focus products](#).

# November 2024 updates

## Updated Vulnerability Mappings

- Snort / Sourcefire 31470 updated Bugtraq, CVE, Nessus
- Juniper IDP update 3757 updated CVE
- TippingPoint UnityOne DV9967 updated CVE
- Symantec Network Security 7100 1972 updated Bugtraq
- Palo Alto Networks PAN-OS 11.2 updated CVE

## Updated Geographic Information

The Geographic Information version is **GeoIP-532\_20241115**.

## File Name

**ArcSight\_Context\_Update\_November\_2024.1115\_070710.zip**

For instructions about installing the Context updates on ESM and Logger, see [Installation Guides for Content and Context Updates](#).

# October 2024 updates

## Updated Vulnerability Mappings

- Snort / Sourcefire 31470 updated CVE
- Juniper IDP update 3747 updated CVE
- TippingPoint UnityOne DV9952 updated CVE
- Symantec Network Security 7100 1949 updated Bugtraq
- Palo Alto Networks PAN-OS 10.0.8 updated CVE

## Updated Geographic Information

The Geographic Information version is **GeoIP-532\_2024109**.

## File Name

**ArcSight\_Context\_Update\_October\_2024.1009\_092227.zip**

For instructions about installing the Context updates on ESM and Logger, see [Installation Guides for Content and Context Updates](#).

# September 2024 updates

## Updated Vulnerability Mappings

- Snort / Sourcefire 31470 updated CVE
- Juniper IDP update 3739 updated CVE
- TippingPoint UnityOne DV9940 updated CVE
- Palo Alto Networks PAN-OS 10.0.8 updated CVE

## Updated Geographic Information

The Geographic Information version is **GeoIP-532\_20240911**.

### File Name

**ArcSight\_Context\_Update\_September\_2024.0911\_092916.zip**

For instructions about installing the Context updates on ESM and Logger, see [Installation Guides for Content and Context Updates](#).

# August 2024 updates

## Updated Vulnerability Mappings

- Snort / Sourcefire 31470 updated CVE
- Juniper IDP update 3729 updated CVE
- TippingPoint UnityOne DV9931 updated CVE

## Updated Geographic Information

The Geographic Information version is **GeoIP-532\_20240815**.

## File Name

**ArcSight\_Context\_Update\_August\_2024.0814\_031010.zip**

For instructions about installing the Context updates on ESM and Logger, see [Installation Guides for Content and Context Updates](#).

# July 2024 Updates

## Updated Vulnerability Mappings

- Snort / Sourcefire 31470 updated Bugtraq, CVE
- Juniper IDP update 3722 updated CVE
- TippingPoint UnityOne DV9922 updated CVE
- Symantec Network Security 7100 1891 updated Bugtraq
- Palo Alto Networks PAN-OS 10.0.8 updated CVE

## Updated Geographic Information

The Geographic Information version is **GeoIP-532\_20240717**.

## File Name

**ArcSight\_Context\_Update\_July\_2024.0717\_023613.zip**

For instructions about installing the Context updates on ESM and Logger, see [Installation Guides for Content and Context Updates](#).

# June 2024 Updates

## Updated Vulnerability Mappings

- Snort / Sourcefire 31470 updated Bugtraq, CVE, MSSB
- Juniper IDP update 3712 updated CVE
- TippingPoint UnityOne DV9912 updated CVE
- Symantec Network Security 7100 1871 updated Bugtraq

## Updated Geographic Information

The Geographic Information version is **GeoIP-532\_20240613**.

### File Name

**ArcSight\_Context\_Update\_June\_2024.0613\_113412.zip**

For instructions about installing the Context updates on ESM and Logger, see [Installation Guides for Content and Context Updates](#).

# May 2024 Updates

## Updated Vulnerability Mappings

- Snort / Sourcefire 31470 updated CVE
- Juniper IDP update 3703 updated CVE
- TippingPoint UnityOne DV9899 updated CVE
- Palo Alto Networks PAN-OS 10.0.8 updated CVE
- McAfee Network Security Manager 11.10.14.4 updated CVE
- Fortinet Fortigate 5.2 Content 3.086 updated CVE

## Updated Geographic Information

The Geographic Information version is **GeoIP-532\_20240515**.

## File Name

**ArcSight\_Context\_Update\_May\_2024.0515\_015820.zip**

For instructions about installing the Context updates on ESM and Logger, see [Installation Guides for Content and Context Updates](#).

# April 2024 Updates

## Updated Vulnerability Mappings

- Snort / Sourcefire 31470 updated CVE
- Juniper IDP update 3692 updated CVE
- TippingPoint UnityOne DV9892 updated CVE
- Symantec Network Security 7100 1824 updated Bugtraq, Nessus, CERT
- Palo Alto Networks PAN-OS 10.0.8 updated CVE

## Updated Geographic Information

The Geographic Information version is **GeoIP-532\_20240410**.

## File Name

**ArcSight\_Context\_Update\_April\_2024.0410\_014720.zip**

For instructions about installing the Context updates on ESM and Logger, see [Installation Guides for Content and Context Updates](#).

# March 2024 Updates

## Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3684 updated CVE
- McAfee Intrushield 11.10.14.4 updated Faultline, CVE, Nessus
- TippingPoint UnityOne DV9882 updated CVE
- Palo Alto Networks PAN-OS 10.0.8 updated CVE

## Updated Geographic Information

The Geographic Information version is **GeoIP-532\_20240313**.

## File Name

**ArcSight\_Context\_Update\_March\_2024.0313\_104929.zip**

For instructions about installing the Context updates on ESM and Logger, see [Installation Guides for Content and Context Updates](#).

# February 2024 Updates

## Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3676 updated CVE
- McAfee Intrushield 11.10.13.7 updated CVE
- TippingPoint UnityOne DV9874 updated CVE

## Updated Geographic Information

The Geographic Information version is **GeoIP-532\_20240215**.

### File Name

**ArcSight\_Context\_Update\_February\_2024.0214\_114422.zip**

For instructions about installing the Context updates on ESM and Logger, see [Installation Guides for Content and Context Updates](#).

# January 2024 Updates

## Updated Vulnerability Mappings

- Snort / Sourcefire 31470 updated CVE
- Juniper IDP update 3669 updated CVE
- McAfee Intrushield 11.10.13.3 updated CVE
- TippingPoint UnityOne DV9865 updated CVE
- Palo Alto Networks PAN-OS 10.0.8 updated CVE
- Fortinet FortiProxy 7.2.6 updated CVE

## Updated Geographic Information

The Geographic Information version is **GeoIP-532\_20240117**.

## File Name

**ArcSight\_Context\_Update\_January\_2024.0117\_021138.zip**

For instructions about installing the Context updates on ESM and Logger, see [Installation Guides for Content and Context Updates](#).

# Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

**Feedback on Release Notes for Context - GeoLocation & Vulnerability Signature Updates 2024 (SmartConnectors 8.4.x)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [MFI-Documentation-Feedback@opentext.com](mailto:MFI-Documentation-Feedback@opentext.com).

We appreciate your feedback!