opentext™

ArcSight SmartConnectors

Software Version: 8.4.x

Release Notes for Context-GeoLocation & Vulnerability Signature Updates 2023

Document Release Date: 2023
Software Release Date: 2023

Legal Notices

Open Text Corporation

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

Copyright Notice

Trademark Notices

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 2023

This guide provides information for all the monthly Release Updates for **ArcSight Context-GeoLocation & Vulnerability Signature for the year 2023**.

Note: From May 2023 onwards, the ArcSight Context-GeoLocation & Vulnerability Signature updates will be a monthly release.

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.

For specific product issues, contact Open Text Support for Micro Focus products.

October 2023 Updates

Updated Vulnerability Mappings

- Snort / Sourcefire 31470 updated CVE
- Juniper IDP update 3641 updated CVE
- McAfee Intrushield 11.10.10.2 updated CVE
- TippingPoint UnityOne DV9832 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20231020**.

File Name

ArcSight_Context_Update_October_2023.1020_091754.zip

For instructions about installing the Context updates on ESM and Logger, see Installation Guides for Content and Context Updates.

September 2023 Updates

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE, MSSB
- Juniper IDP update 3635 updated CVE
- McAfee Intrushield 11.10.9.4 updated CVE
- TippingPoint UnityOne DV9828 updated Bugtraq, CVE, Nessus
- Palo Alto Networks PAN-OS 10.0.8 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_2023105**.

File Name

ArcSight_Context_Update_October_2023.1005_010347.zip

For instructions about installing the Context updates on ESM and Logger, see Installation Guides for Content and Context Updates.

August 2023 Updates

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3622 updated CVE
- McAfee Intrushield 11.10.8.1 updated CVE
- TippingPoint UnityOne DV9814 updated CVE
- Palo Alto Networks PAN-OS 10.0.8 updated CVE
- McAfee Group Shield Enterprise 7.0 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_2023089**.

File Name

ArcSight_Context_Update_August_2023.0809_103057.zip

For instructions about installing the Context updates on ESM and Logger, see Installation Guides for Content and Context Updates.

July 2023 Updates

Updated Vulnerability Mappings

- Snort / Sourcefire 31470 updated CVE
- Juniper IDP update 3618 updated CVE
- McAfee Intrushield 11.10.7.4 updated CVE
- TippingPoint UnityOne DV9811 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20230728**.

File Name

ArcSight_Context_Update_July_2023.0718_112536.zip

For instructions about installing the Context updates on ESM and Logger, see Installation Guides for Content and Context Updates.

June 2023 Updates

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3604 updated CVE
- McAfee Intrushield 11.10.6.1 updated CVE
- TippingPoint UnityOne DV9800 updated CVE
- Symantec Network Security DV9800 updated Bugtraq
- Palo Alto Networks PAN-OS 10.0.8 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20230614**.

File Name

ArcSight_Context_Update_June_2023.0614_013436.zip

For instructions about installing the Context updates on ESM and Logger, see Installation Guides for Content and Context Updates.

May 2023 Updates

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3596 updated CVE
- McAfee Intrushield 11.10.5.1 updated CVE
- TippingPoint UnityOne DV9788 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20230510**.

File Name

ArcSight_Context_Update_May_2023.0510_112643.zip

For instructions about installing the Context updates on ESM and Logger, see Installation Guides for Content and Context Updates.

April 2023 Updates

R2

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3592 updated CVE
- McAfee Intrushield 11.9.4.3 updated CVE
- TippingPoint UnityOne DV9784 updated Bugtraq, CVE
- Symantec Network Security DV9784 updated Bugtraq
- Palo Alto Networks PAN-OS 10.0.8 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20230426**.

File Name

ArcSight_Context_Update_April_2023.0426_031250.zip

R1

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3585 updated CVE
- McAfee Intrushield 11.9.4.1 updated CVE
- TippingPoint UnityOne DV9780 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20230413**.

File Name

ArcSight_Context_Update_April_2023.0413_103535.zip

For instructions about installing the Context updates on ESM and Logger, see Installation Guides for Content and Context Updates.

March 2023 Updates

R2

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3581 updated Faultline, CVE, Nessus
- McAfee Intrushield 11.9.3.3 updated CVE
- TippingPoint UnityOne DV9773 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20230322**.

File Name

ArcSight_Context_Update_March_2023.0322_011153.zip

R1

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3576 updated Faultline, CVE, Nessus
- McAfee Intrushield 11.9.2.5 updated CVE
- TippingPoint UnityOne DV9767 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_2023038**.

File Name

ArcSight_Context_Update_March_2023.0308_101515.zip

For instructions about installing the Context updates on ESM and Logger, see Installation Guides for Content and Context Updates.

February 2023 Updates

R2

Updated Vulnerability Mappings

Snort / Sourcefire 2983 updated CVE

Juniper IDP update 3573 updated CVE

McAfee Intrushield 11.9.2.2 updated CVE

TippingPoint UnityOne DV9763 updated CVE

Symantec Network Security DV9763 updated Bugtraq

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20230222**.

File Name

ArcSight_Context_Update_February_2023.0222_010221.zip

R1

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3569 updated CVE
- McAfee Intrushield 11.9.1.5 updated CVE
- TippingPoint UnityOne DV9759 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_2023028**.

File Name

ArcSight_Context_Update_February_2023.0208_090936.zip

For instructions about installing the Context updates on ESM and Logger, see Installation Guides for Content and Context Updates.

January 2023 Updates

R2

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3565 updated CVE
- McAfee Intrushield 10.9.41.3 updated CVE
- TippingPoint UnityOne DV9756 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20230125**.

File Name

ArcSight_Context_Update_January_2023.0125_103938.zip

R1

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3560 updated CVE
- McAfee Intrushield 10.9.41.1 updated CVE
- TippingPoint UnityOne DV9751 updated CVE
- IBM Security Network Protection 4212.12221 updated X-Force

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20230111**.

File Name

ArcSight_Context_Update_January_2023.0111_084226.zip

For instructions about installing the Context updates on ESM and Logger, see Installation Guides for Content and Context Updates.

January 2023 Updates

R2

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3565 updated CVE
- McAfee Intrushield 10.9.41.3 updated CVE
- TippingPoint UnityOne DV9756 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20230125**.

File Name

ArcSight_Context_Update_January_2023.0125_103938.zip

R1

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3560 updated CVE
- McAfee Intrushield 10.9.41.1 updated CVE
- TippingPoint UnityOne DV9751 updated CVE
- IBM Security Network Protection 4212.12221 updated X-Force

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20230111**.

File Name

ArcSight_Context_Update_January_2023.0111_084226.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 2023 (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.

We appreciate your feedback!