Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3

Release Notes for Context-GeoLocation & Vulnerability Signature Updates 2022

Document Release Date: 2022
Software Release Date: 2022

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

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

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Document Revision History

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

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

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

Document Changes

Date	Product Version	Description
MM/DD/YYYY	X.X.X.X	Description of change

Release Notes for ArcSight Context-GeoLocation & Vulnerability Signature Updates

This guide provides Release Notes for ArcSight Context-GeoLocation & Vulnerability Signature Updates.

Context Update which is also known as ArcSight Context-GeoLocation & Vulnerability Signature Updates is delivered through ESM and Logger SKUs, once every two weeks. 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.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight 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.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors.

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 Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care.

November 2022 Updates

R1

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3542 updated CVE
- McAfee Intrushield 10.9.39.1 updated CVE
- TippingPoint UnityOne DV9730 updated CVE
- IBM Security Network Protection 4207.21164 updated X-Force

Updated Geographic Information

The Geographic Information version is **GeoIP-532_2022119**.

File Name

ArcSight_Context_Update_November_2022.1109_033024.zip

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

October 2022 Updates

R2

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3539 updated CVE
- McAfee Intrushield 10.9.38.4 updated CVE
- TippingPoint UnityOne DV9724 updated Bugtraq, CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20221027**.

File Name

ArcSight_Context_Update_October_2022.1027_020049.zip

R1

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3534 updated CVE
- McAfee Intrushield 10.9.38.2 updated CVE
- TippingPoint UnityOne DV9718 updated CVE
- IBM Security Network Protection 4207.21164 updated X-Force
- Palo Alto Networks PAN-OS 10.0.8 updated CVE
- 7.0 updated CVE, X-Force

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20221013**.

File Name

ArcSight_Context_Update_October_2022.1013_032952.zip

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

September 2022 Updates

R2

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3527 updated CVE
- McAfee Intrushield 10.9.37.3 updated CVE
- TippingPoint UnityOne DV9711 updated CVE
- IBM Security Network Protection 4207.21164 updated X-Force

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20220923**.

File Name

ArcSight_Context_Update_September_2022.0922_051651.zip

R1

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3523 updated CVE
- McAfee Intrushield 10.9.36.8 updated CVE
- TippingPoint UnityOne DV9708 updated CVE
- Symantec Network Security DV9708 updated Bugtraq

Updated Geographic Information

The Geographic Information version is **GeoIP-532_2022098**.

File Name

ArcSight_Context_Update_September_2022.0908_015302.zip

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

August 2022 Updates

R2

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3520 updated CVE
- McAfee Intrushield 10.9.36.5 updated CVE
- TippingPoint UnityOne DV9705 updated CVE
- IBM Security Network Protection 4207.21164 updated X-Force

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20220825**.

File Name

ArcSight_Context_Update_August_2022.0825_034041.zip

R1

Updated Vulnerability Mappings

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3513 updated CVE
- McAfee Intrushield 10.9.36.2 updated CVE
- TippingPoint UnityOne DV9700 updated CVE
- IBM Security Network Protection 4207.21164 updated X-Force
- Palo Alto Networks PAN-OS 10.0.8 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20220811**.

File Name

ArcSight_Context_Update_August_2022.0811_052621.zip

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

July 2022 Updates

R2

Updated Vulnerability Mappings

This release contains updated vulnerability mapping for:

- Snort / Sourcefire 2983 updated Faultline, Bugtraq, CVE, Nessus, MSSB
- Juniper IDP update 3513 updated CVE
- McAfee Intrushield 10.9.35.4 updated CVE
- TippingPoint UnityOne DV9696 updated Faultline, CVE, MSSB
- IBM Security Network Protection 4207.21164 updated X-Force

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20220729**.

File Name

ArcSight_Context_Update_July_2022.0729_120537.zip

R1

Updated Vulnerability Mappings

This release contains updated vulnerability mapping for:

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3508 updated CVE
- McAfee Intrushield 10.9.35.1 updated CVE
- TippingPoint UnityOne DV9692 updated CVE
- IBM Security Network Protection 4207.07191 updated X-Force

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20220714**.

File Name

ArcSight_Context_Update_July_2022.0714_105201.zip

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

June 2022 Updates

R2

Updated Vulnerability Mappings

This release contains updated vulnerability mappings for:

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3503 updated CVE
- McAfee Intrushield 10.9.34.2 updated CVE
- TippingPoint UnityOne DV9687 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20220628**.

File Name

ArcSight_Context_Update_June_2022.0628_121439.zip

R1

Updated Vulnerability Mappings

This release contains updated vulnerability mappings for:

- Snort / Sourcefire 2983 updated Bugtraq, MSSB, CVE
- Juniper IDP update 3495 updated Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB
- McAfee Intrushield 10.9.33.3 updated CVE
- TippingPoint UnityOne DV9678 updated CVE
- IBM Security Network Protection 4205.19171 updated X-Force

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20220530**.

File Name

ArcSight_Context_Update_June_2022.0617_090713.zip

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

May 2022 Updates

R2

Updated Vulnerability Mappings

This release contains updated vulnerability mappings for:

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3500 updated CVE
- McAfee Intrushield 10.9.34.1 updated CVE
- TippingPoint UnityOne DV9678 updated CVE
- IBM Security Network Protection 4205.19171 updated X-Force

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20220617**.

File Name

ArcSight_Context_Update_June_2022.0617_090713.zip

R1

Updated Vulnerability Mappings

This release contains updated vulnerability mappings for:

- Snort / Sourcefire 2983 updated CVE, MSSB
- Juniper IDP update 3490 updated CVE
- McAfee Intrushield 10.9.33.2 updated CVE, Nessus
- TippingPoint UnityOne DV9664 updated CVE
- IBM Security Network Protection 3240 updated X-Force
- Palo Alto Networks PAN-OS 10.0.8 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20220513**.

File Name

ArcSight_Context_Update_May_2022.0512_055702.zip

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

April 2022 Updates

R2

Updated Vulnerability Mappings

This release contains updated vulnerability mappings for:

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3485 updated CVE
- McAfee Intrushield 10.9.32.3 updated Faultline, CVE
- TippingPoint UnityOne DV9655 updated Bugtraq, CVE
- McAfee HIPS 7.0/8.0 content version 12138 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20220428**.

File Name

ArcSight_Context_Update_April_2022.0428_010035.zip

R1

Updated Vulnerability Mappings

This release contains updated vulnerability mappings for:

- Snort / Sourcefire 31210 updated CVE
- Juniper IDP update 3480 updated CVE
- TippingPoint UnityOne DV9655 updated Bugtraq, CVE
- Palo Alto Networks PAN-OS 10.0.8 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_2022046**.

File Name

ArcSight_Context_Update_April_2022.0406_025405.zip

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

April 2022 Updates

R2

Updated Vulnerability Mappings

This release contains updated vulnerability mappings for:

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3485 updated CVE
- McAfee Intrushield 10.9.32.3 updated Faultline, CVE
- TippingPoint UnityOne DV9655 updated Bugtraq, CVE
- McAfee HIPS 7.0/8.0 content version 12138 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20220428**.

File Name

ArcSight_Context_Update_April_2022.0428_010035.zip

R1

Updated Vulnerability Mappings

This release contains updated vulnerability mappings for:

- Snort / Sourcefire 31210 updated CVE
- Juniper IDP update 3480 updated CVE
- TippingPoint UnityOne DV9655 updated Bugtraq, CVE
- Palo Alto Networks PAN-OS 10.0.8 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_2022046**.

File Name

ArcSight_Context_Update_April_2022.0406_025405.zip

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

March 2022 Updates

R2

Updated Vulnerability Mappings

This release contains updated vulnerability mappings for:

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3474 updated CVE
- TippingPoint UnityOne DV9649 updated Bugtraq, CVE
- IBM Security Network Protection 3240 updated X-Force

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20220323**.

File Name

ArcSight_Context_Update_March_2022.0323_110650.zip

R1

Updated Vulnerability Mappings

This release contains updated vulnerability mappings for:

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3470 updated CVE
- McAfee Intrushield 10.9.31.1 updated CVE
- TippingPoint UnityOne DV9647 updated Bugtraq, CVE
- Palo Alto Networks PAN-OS 10.0.8 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20220316**.

File Name

ArcSight_Context_Update_March_2022.0316_083757.zip

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

February 2022 Updates

R2

Updated Vulnerability Mappings

This release contains updated vulnerability mappings for:

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3468 updated CVE
- McAfee Intrushield 10.9.30.4 updated CVE
- TippingPoint UnityOne DV9639 updated Bugtraq, CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_2022031**.

File Name

ArcSight_Context_Update_February_2022.0301_104227.zip

R1

Updated Vulnerability Mappings

This release contains updated vulnerability mappings for:

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3465 updated CVE
- McAfee Intrushield 10.8.30.1 updated CVE
- TippingPoint UnityOne DV9636 updated CVE
- IBM Security Network Protection updated X-Force
- McAfee HIPS 7.0/8.0 content version 12052 updated CVE
- Palo Alto Networks PAN-OS 10.0.8 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20220215**.

File Name

ArcSight_Context_Update_February_2022.0215_070331.zip

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

January 2022 Updates

R2

Updated Vulnerability Mappings

This release contains updated vulnerability mappings for:

- Snort / Sourcefire 2983 updated CVE
- Juniper IDP update 3460 updated CVE
- McAfee Intrushield 10.8.29.5 updated CVE
- TippingPoint UnityOne DV9632 updated CVE
- IBM Security Network Protection updated X-Force

Updated Geographic Information

The Geographic Information version is **GeoIP-532_2022022**.

File Name

ArcSight_Context_Update_February_2022.0202_121807.zip

R1

Updated Vulnerability Mappings

This release contains updated vulnerability mappings for:

- Snort / Sourcefire 2983 updated Faultline, Bugtraq, CVE, Nessus
- Juniper IDP update 3456 updated CVE, Nessus
- McAfee Intrushield 10.8.29.3 updated CVE
- TippingPoint UnityOne DV9630 updated CVE
- IBM Security Network Protection updated X-Force
- McAfee HIPS 7.0/8.0 content version 12015 updated CVE

Updated Geographic Information

The Geographic Information version is **GeoIP-532_20220114**.

File Name

ArcSight_Context_Update_January_2022.0114_041935.zip

For instructions about installing the Context updates on ESM and Logger, seeInstallation 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 2022 (SmartConnectors 8.3)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!