

RSA® ARCHER®
GRC Platform
Implementation Guide

Digital Defense Frontline VM 6.0

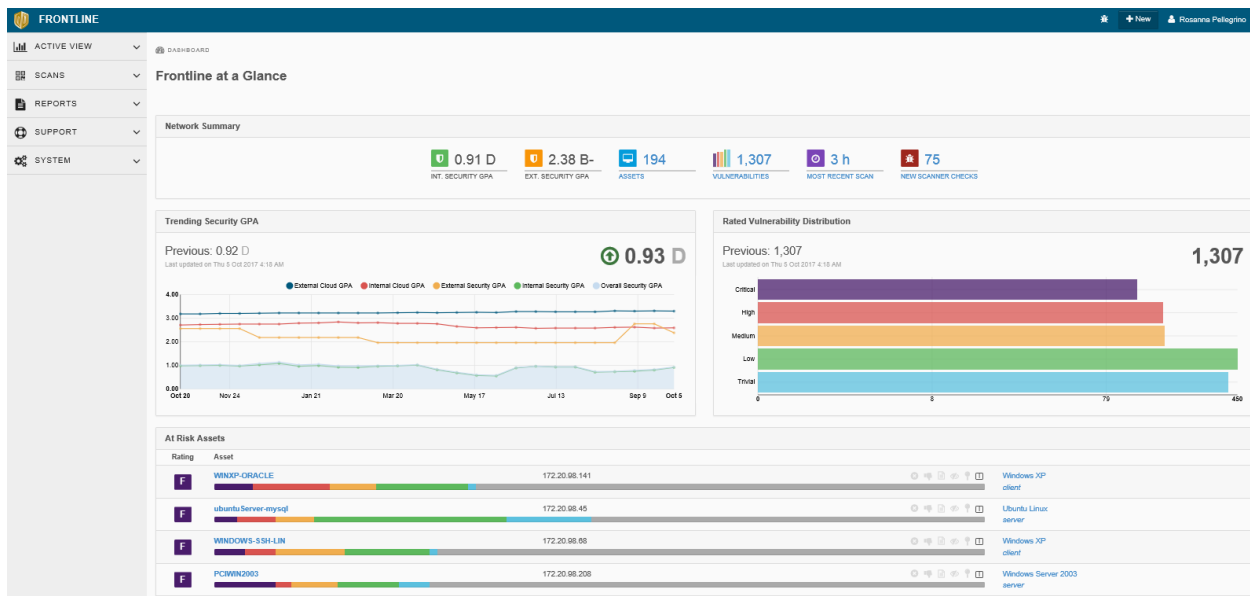
Jeffrey Carlson, RSA Partner Engineering
Last Modified: October 16th, 2017

Solution Summary

Digital Defense's Frontline Vulnerability Manager™ (Frontline VM) is the industry's most comprehensive, accurate, and easy to use vulnerability management software. Backed by security research expertise (DDI VRT™), and a highly intuitive user interface touted by customers as simple, insightful, and immediately actionable, Frontline VM delivers unparalleled excellence from deep, accurate network and host assessments all the way to intelligent integration with SIEMs and security workflow management systems. Together, Frontline RNA™ and Frontline VM yield the industry's lowest false positive rate – critical to effective vulnerability discovery, productive remediation guidance, and ultimately, true cyber risk reduction.

The Digital Defense Frontline VM integration with RSA Archer allows you to combine the power of Frontline's device discovery and vulnerability detection with RSA's Vulnerability Management features to view your devices and their vulnerabilities in the context of the business risk they pose to your organization.

Partner Integration Overview	
RSA Archer Solution	IT Security Vulnerabilities Program
RSA Archer Use Case	IT Security Risk Management
RSA Archer Applications	Vulnerability Scan Results, Devices
Uses Custom Application	No
Requires On-Demand License	No



Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Digital Defense Frontline VM with the RSA Archer GRC Platform. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

!> Important: The integration described in this guide is being provided as a reference implementation for evaluation and testing purposes. It may or may not meet the needs and use cases for your organization. If additional customizations or enhancements are needed, it is recommended that customers contact RSA Professional Services for assistance.

Digital Defense Frontline VM Configuration

By integrating Digital Defense Frontline VM with RSA Archer, organizations can derive the following benefits:

- **Complete an accurate detailed analysis of devices on network via integration**

The end user will be able to take advantage of Digital Defense's scan-to-scan host correlation combined with the functionality of the RSA products. Digital Defense's scan-to-scan host correlation ensures that RSA products receive the most accurate and up-to-date information about hosts that have been scanned, allowing the user to make better, more informed decisions when coupled with information presented by the McAfee products.

Digital Defense's scan to scan host correlation identifies over 25 host characteristics that also include applications that are installed on the host, which helps our mutual customers insure that their host security investments are protecting the environment and data.

- **Deliver an effective path to remediation**

Effectively improve risk posture, remediation efforts identified and prioritized help plan remediation thru recommendations with rule based policies within RSA Archer.

- **Communicate, collaborate and transform**

Ever changing breach landscape, counter measures can be deployed based on risk evaluation information contextualized by Frontline and integrated within RSA Archer.

Before integrating Frontline VM with RSA Archer it is first necessary to generate an API key. Perform the steps below to do so.

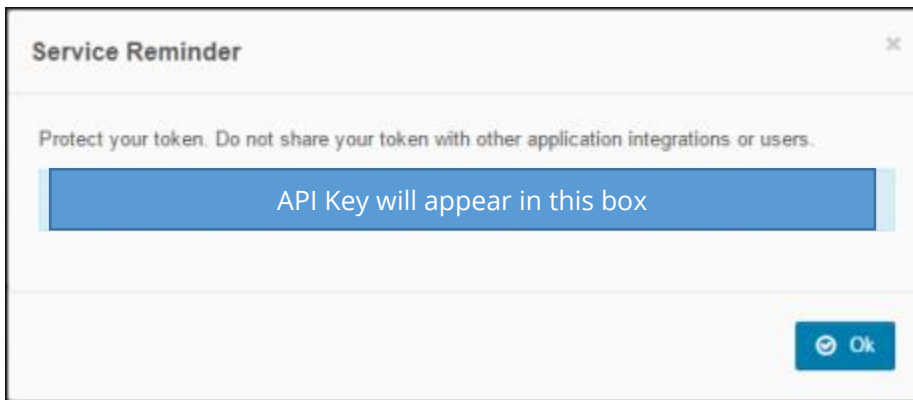
Generate Frontline VM API Key

The following instructions describe how to generate an API key to access Frontline VM data.

To generate a **Frontline VM** API key:

1. Log in to Frontline VM.
2. In the site header, select your name and choose **My profile**.
3. On the **API Tokens** tab, select **Create new token**.
4. In the **Add New Token** dialog, type the token name (it can be whatever you like) and select **OK**.
5. Your token is created.

Below your token name, **Click to show key** displays your API key, which you need to integrate Frontline VM with RSA Archer.



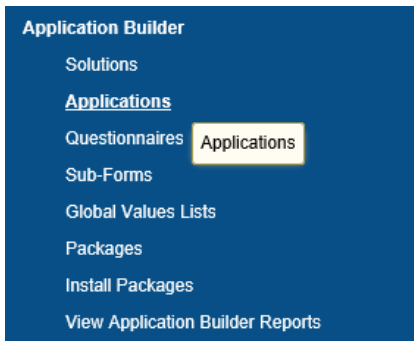
Note: An API key is equivalent to a user's password. Do not use a key with more than one product integration. If you believe a key is compromised, delete the token from Frontline VM immediately by selecting and the resulting checkmark to confirm.

RSA Archer GRC Configuration

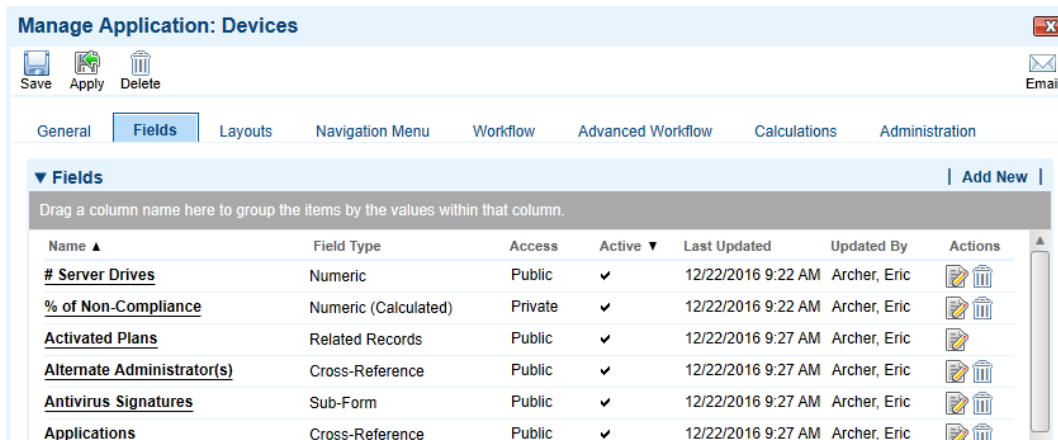
Configuring the Devices Application

Before importing the necessary data feeds for importing vulnerability information, it is first necessary to make a number of changes to the existing Devices application within Archer. To add the **DDI Device ID** field to the **Devices** application perform the following steps:

1. Click the down arrow next to the tools icon in the menu bar.
2. In the **Application Builder** section, choose **Applications**:



3. Choose the **Devices** application name from the list.
4. Click on the **Fields** tab next to **General**.
5. Click on the **Add New** link in the upper right of the **fields** table:

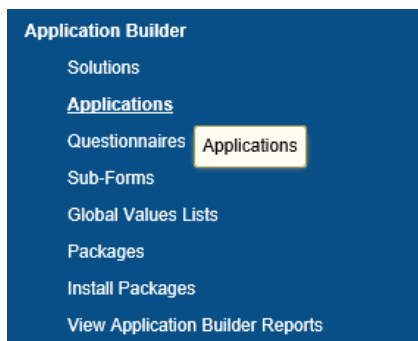


6. Choose the **Create a new Field from scratch** radio button.
7. Choose the **Text** field type. Click **OK**.
8. Enter **DDI Device ID** for the name. Complete any other fields required by your organization.
9. Click **Save** above the **General** tab.

Configuring the Vulnerability Scan Results Application

Before importing the necessary data feeds for importing vulnerability information, it is first necessary to make a number of changes to the existing Devices application within Archer. To add the **DDI Vuln Instance ID** field to the **Vulnerability Scan Results** application perform the following steps:

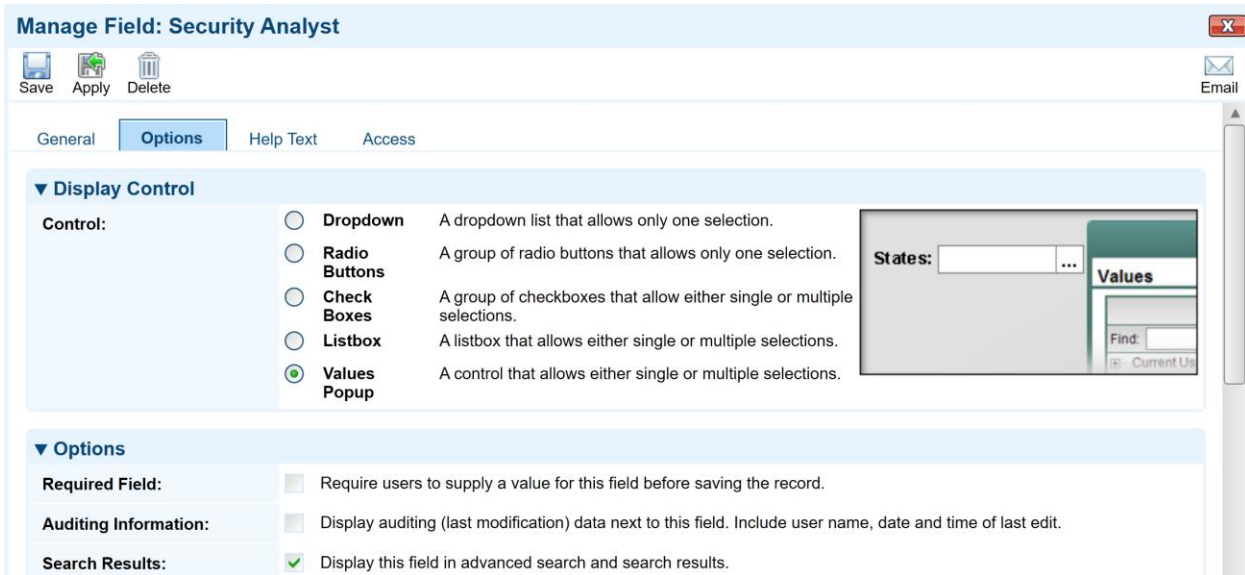
1. Click the down arrow next to the tools icon in the menu bar.
2. In the **Application Builder** section, choose **Applications**:



3. Choose the **Vulnerability Scan Results** application name from the list.
4. Click on the **Fields** tab next to **General**.
5. Click on the **Add New** link in the upper right of the **fields** table:
6. Choose the **Create a new Field from scratch** radio button.
7. Choose the **Text** field type. Click **OK**.
8. Enter **DDI Vuln Instance ID** for the name. Complete any other fields required by your organization.
9. Click **Save** above the **General** tab.

As part of the integration it is also necessary to mark the **Security Analyst** field as **not required** in order for the Data Feed to run without errors. To do this, perform the following steps:

1. Follow steps 1-4 above
2. Click on the **Security Analyst** field in the fields table.
3. Choose the **Options** tab. In the **Options** section of the page, **uncheck** the box next to **Required Field**.

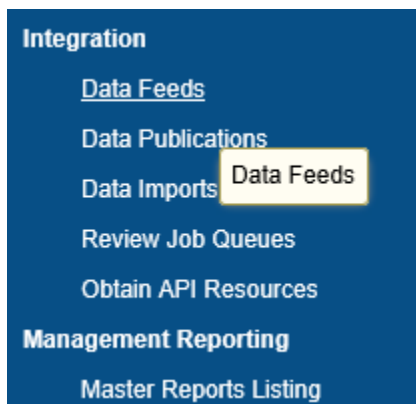


4. Click **Save** above the **General** tab.

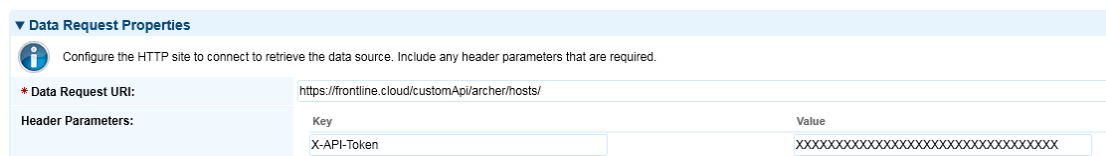
Importing and Configuring the Frontline VM Devices Data Feed

Digital Defense Device records are created in RSA Archer via a preconfigured Data Feed. This Data Feed loads the host information from an XML file that is pulled from the Digital Defense APIs using a customer-specific API key. To configure the Data Feed, perform the following steps:

1. On your RSA Archer Server, browse to **Administration -> Integration -> Data Feeds**:

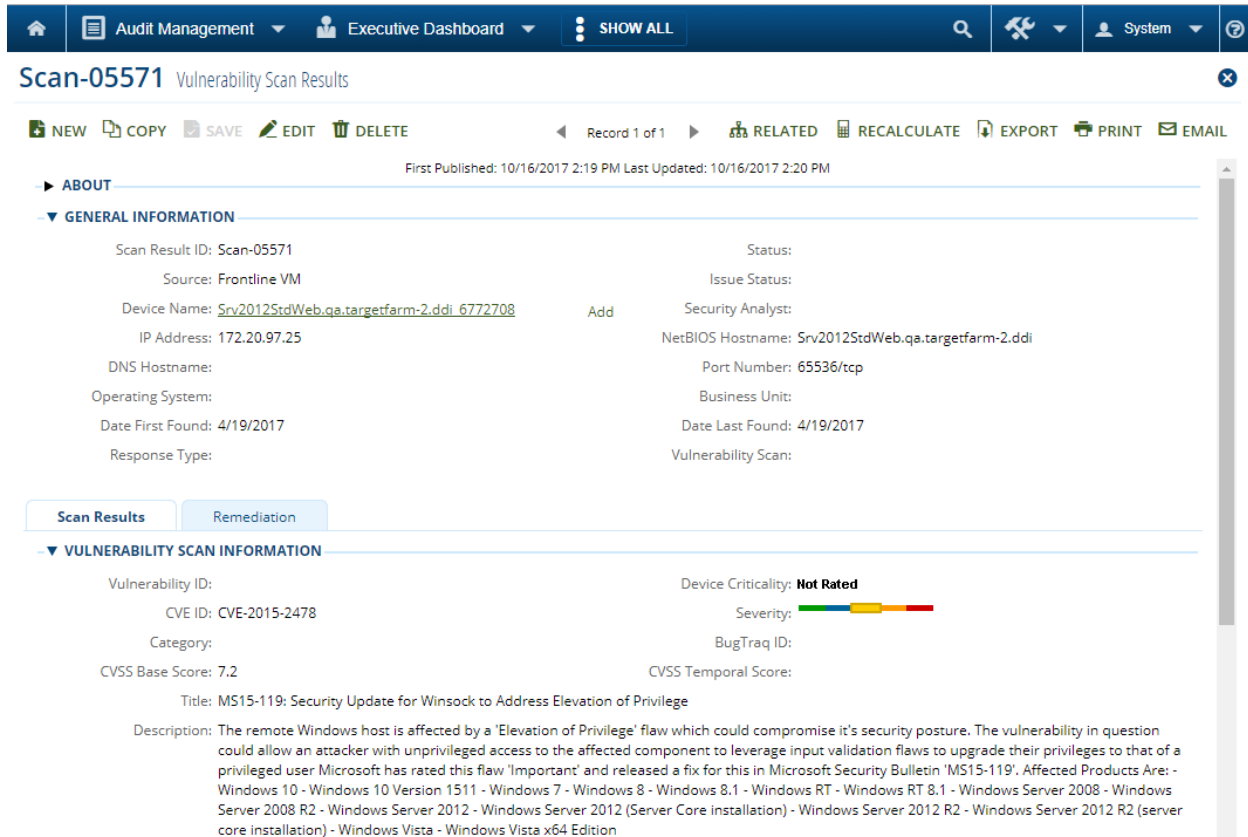


2. Select **Import** and browse to the Data Feed file (Digital_Defense_Frontline_VM_Devices.dfx5).
3. Click on the **Transport** tab.
4. In the **Data Request Properties** section, locate the Header Parameter **X-API-Token**. Replace the Xs in the **Value** field with your Frontline VM API Token.



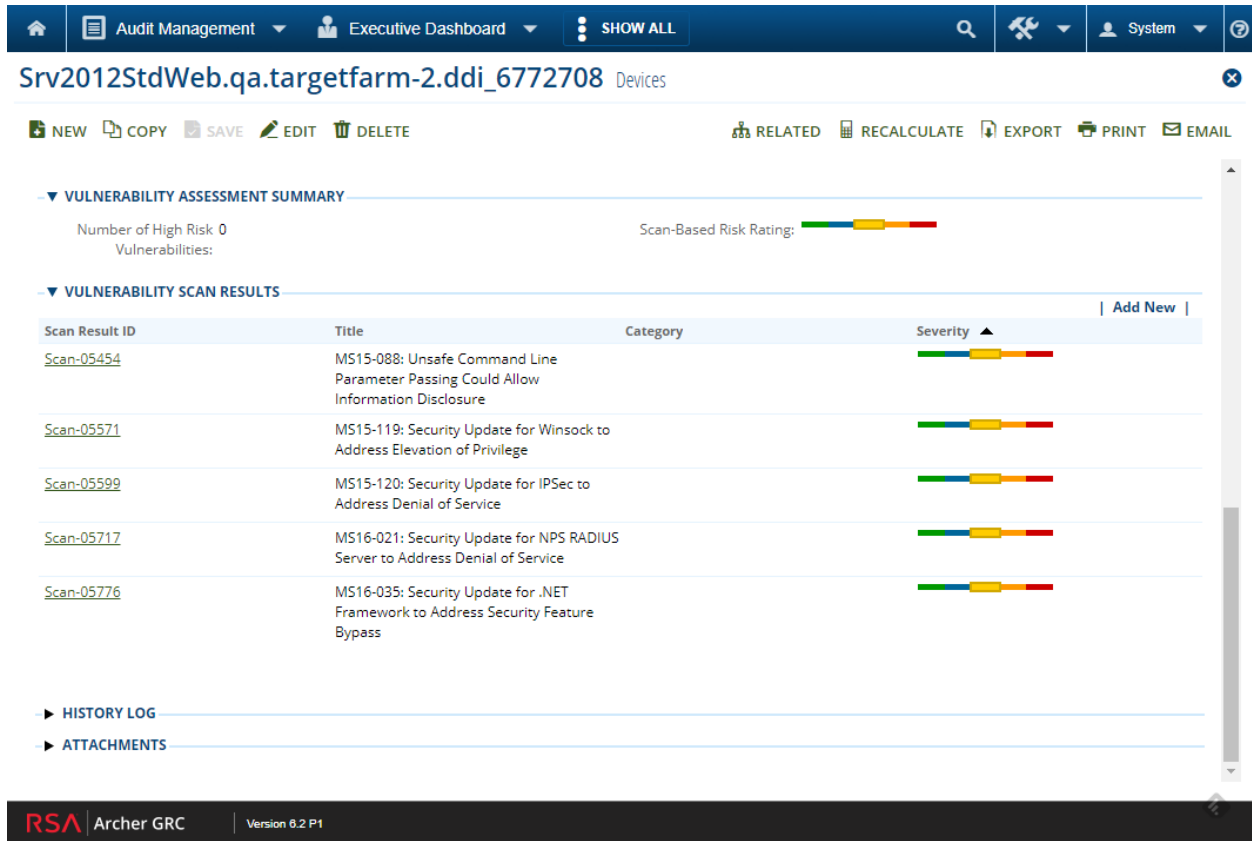
Using Frontline VM with RSA Archer

The integration of Digital Defense Frontline VM with RSA Archer IT Security Risk Management enables customers to have a complete analysis of digital asset within their environment an accurate view of the risks. Organizations can proactively identify, track status and manage the repair of critical vulnerabilities.



The screenshot displays the 'Scan-05571 Vulnerability Scan Results' page. The interface includes a top navigation bar with 'Audit Management', 'Executive Dashboard', and 'SHOW ALL'. Below the navigation, there are action buttons: NEW, COPY, SAVE, EDIT, DELETE, and a record indicator 'Record 1 of 1'. Further actions include RELATED, RECALCULATE, EXPORT, PRINT, and EMAIL. The page is divided into sections: 'ABOUT' (with 'First Published: 10/16/2017 2:19 PM Last Updated: 10/16/2017 2:20 PM'), 'GENERAL INFORMATION', and 'VULNERABILITY SCAN INFORMATION'. The 'GENERAL INFORMATION' section lists details such as Scan Result ID (Scan-05571), Source (Frontline VM), Device Name (Srv2012StdWeb.qa.targetfarm-2.ddi.6772708), IP Address (172.20.97.25), DNS Hostname, Operating System, Date First Found (4/19/2017), and Response Type. The 'VULNERABILITY SCAN INFORMATION' section shows Vulnerability ID, CVE ID (CVE-2015-2478), Category, CVSS Base Score (7.2), Device Criticality (Not Rated), Severity (visualized as a bar chart), BugTraq ID, and CVSS Temporal Score. A detailed description of the vulnerability is provided at the bottom.


Having the ability to know and report what devices are on your network and how they are vulnerable allows organizations to manage business critical hosts. With the consolidated view, the individual risks can be mapped to multiple hosts, and in addition knowing what vulnerabilities are found within each hosts.








Srv2012StdWeb.qa.targetfarm-2.ddi_6772708 Devices

NEW COPY SAVE EDIT DELETE RELATED RECALCULATE EXPORT PRINT EMAIL

VULNERABILITY ASSESSMENT SUMMARY

Number of High Risk 0 Vulnerabilities: Scan-Based Risk Rating: 

VULNERABILITY SCAN RESULTS | Add New |

Scan Result ID	Title	Category	Severity
Scan-05454	MS15-088: Unsafe Command Line Parameter Passing Could Allow Information Disclosure		
Scan-05571	MS15-119: Security Update for Winsock to Address Elevation of Privilege		
Scan-05599	MS15-120: Security Update for IPSec to Address Denial of Service		
Scan-05717	MS16-021: Security Update for NPS RADIUS Server to Address Denial of Service		
Scan-05776	MS16-035: Security Update for .NET Framework to Address Security Feature Bypass		

HISTORY LOG ATTACHMENTS

RSA Archer GRC | Version 6.2 P1

This many to many relationship gives the RSA Archer Platform an entire vulnerability lifecycle – by providing complete and accurate information for remediation and verification.

Certification Environment for RSA Archer GRC

Date Tested: October 11th, 2017

Certification Environment		
Product Name	Version Information	Operating System
RSA Archer GRC	6.2	Virtual Appliance
Digital Defense Frontline VM	6.0	SaaS

