# Table of Contents

# 1. Technical Advisories

- Technical Advisory #16 - Config Sync may skip steps on Error
- Technical Advisory #17 - PowerScale CSRF Authentication is not compatible with Smartconnect and API services
  Affects Eyeglass releases 2.5.3 and later
- Technical Advisory #18 - Ransomware Defender ECA cluster without Internet access potential for false positives
- Technical Advisory #19 - SMB Data Integrity corner case can leave Deny permission on some or all shares
- Technical Advisory #20 - PowerScale Auditing incorrectly records audit events for paths that do not exist on the cluster when SMB share is mounted with subfolders with a case that does not match the file system
- Technical Advisory #21 - OneFS CLI command bug fails to exit ram
- Technical Advisory #22 - Onefs 8.2 Does not support REST API or SSH SSIP connections from Eyeglass
- Technical Advisory #23 - 2.5.6 Patch 1 Addresses failover Scenario's that can delay some steps from starting immediately
- Technical Advisory #24 Config Only Migration Job deletes shares and exports on the Destination Access Zone
- Technical Advisory #25 OneFS fails to create Quotas with corrupt configuration
- Technical Advisory #26 Eyeglass VM Log4j Hardening
- Technical Advisory #27 - ECA VM Log4j Hardening - (Ransomware Defender, Easy Auditor, Performance Auditor)

- Technical Advisory #28 - Search & Recover, Golden Copy VM Log4j Hardening
- Technical Advisory #29 CVE-2021-45046 log4j (2.16) - Does not apply to any Superna product
- Technical Advisory #30 How to Mitigate Vulnerabilities in JRE 1.8.0_291 in Eyeglass Appliance
- Technical Advisory #31 Ransomware Defender NFS Event Detection Always Enabled in 2.5.8.1-22080/22100

## Technical Advisory #1

For customers where the total number of objects (SMB Shares, NFS Exports, NFS Alias, Quotas) being managed by Superna Eyeglass exceeds 10,000, tasks being performed against the cluster for a large number of objects (such as creating quotas during a failover) may overwhelm the cluster such that not all tasks are completed. An adjustment to the Superna Eyeglass parallel task limit is required. Contact support.superna.net for assistance in updating Eyeglass.

## Technical Advisory #2

In some environments, the memory allocated for the Superna Eyeglass database is not sufficient. In this case Superna Eyeglass no longer functions and the Superna Eyeglass web page windows appear

empty. If you experience this issue, contact support.superna.net for assistance in updating Eyeglass to adjust the memory allocated to the database.

Update April 6, 2016: This issue has been addressed in Eyeglass 1.5.1

## Technical Advisory #3 - reissued April 20

An issue in Eyeglass Release 1.5.0 and 1.5.1 results in duplicate exports being created on the target cluster under certain conditions such as poor connectivity between Eyeglass and the PowerScale cluster. This issue will be addressed in Eyeglass 1.5.2. This issue does not exist in Eyeglass 1.4.8. Eyeglass installations using exports should not upgrade to Eyeglass 1.5.0 or 1.5.1.

Update April 25, 2016: This issue has been addressed in Eyeglass 1.5.2

## Technical Advisory #4 - End of Support for 1.2, 1.3, 1.4 and 1.4.x Releases

All customers running the above releases should upgrade to the latest release using upgrade guide located here. Numerous failover and performance improvements exist in the latest release with all new cases requiring an upgrade.

## Technical Advisory #5 - Incomplete response from PowerScale PAPI may result in deletion of Configuration Objects

Please be advised that we have observed instances where the PowerScale Cluster PAPI used by Eyeglass to collect information becomes unresponsive such that Eyeglass requests for configuration objects are unanswered (for example 503 Service Unavailable). This results in empty Eyeglass inventory for objects that are not retrieved.

Should this happen during scheduled Eyeglass Configuration Replication, it may result in deletion of configuration objects (such as NFS export or SMB shares) from the target cluster. Subsequent cycle with correct response will resolve this situation by creating the configuration objects again.

Should this happen during Eyeglass assisted failover, it may result in deletion of missing configuration objects from both clusters as after the failover the target cluster with missing objects becomes the master active cluster.

The Eyeglass next release will contain defensive code to guard against deletion of configuration objects when the PowerScale PAPI response is incomplete. If you are planning a controlled failover, we ask that you wait and upgrade to 1.5.4 release that blocks PowerScale PAPI errors from impacting a successful failover.
Update May 13, 2016: This issue has been addressed in Eyeglass 1.5.3

## Technical Advisory #6 – Set SyncIQ policies to manual schedule or longer schedule with 1.6 release or risk scheduled jobs running during failover and failing overall Eyeglass failover steps

Following EMC best practices to set SyncIQ policies to manual before any failover KB Article as reference "NOTE: A sync job and failover job cannot run simultaneously by design and will cause the failover attempt to fail. To avoid this condition, set all policies to manual."

Issue: Failover behavior in 1.6 was changed that exposes the window where scheduled policies do not have their scheduled removed in time to prevent them from running in 1.6 release.

This has been addressed in 1.6.3 by having schedules removed and cached at the beginning of the failover and reapplied at the end of the failover.

## Technical Advisory #7 - OneFS 8 BMC firmware bug API call

Please be advised that we have found new case where the BMC firmware bug API call is made under Eyeglass1.6.1 code. This issue has been observed to manifest itself after several days in operation and affects Eyeglass installations where both PowerScale clusters are running OneFS 8. We have switched to a ssh call previously reviewed by EMC and confirmed to not query any BMC APIs in 1.6.x but a left over call in some cases still called this unused API in 1.6.1.

This has been addressed in the 1.6.2 patch such that the BMC firmware bug API is removed. We recommend this new patch release for all Eyeglass patch deployments managing OneFS 8 clusters.

## Technical Advisory #8 - End of Support for 1.5.4 Release

Effective November 1st, 2016 release 1.5.4, All customers running the above releases should upgrade to the latest release using upgrade guide located here. Numerous failover and performance

improvements exist in the latest release with all new cases with this release requiring an upgrade as first resolution step.

## Technical Advisory #9 - Open files Detection on PowerScale

A OneFS issue with open file detection used by Eyeglass in the DR assistant to show open files, only lists files open in system access zone. Other access zones that have open files are not returned by the ISI open files for array command. This means customers can not rely on the open file list in DR assistant to determine open files in none system access zones. No known fix available in any OneFS at this time.

As of release 1.8.1 this feature has been removed with no update or planned availability of a fixed API from Dell EMC.

## Technical Advisory #10 - Uncontrolled Failover Issue when PowerScale Cluster added to Eyeglass with FQDN

Applies to release < 1.8.1 For the case where PowerScale clusters have been added to Eyeglass using FQDN, uncontrolled failover for case where source cluster is not reachable does not start and gives the error ""Error performing zone failover: Cannot find associated source network element for zone".

This issue is addressed in a 1.8.1 patch. Eyeglass installations using FQDN to add clusters must upgrade to this patch once available.

Workaround:
Before an uncontrolled failover where the source cluster is not available, edit the /etc/hosts file on the Eyeglass appliance following the steps below:

1. ssh to the Eyeglass appliance.
2. Assume root user - when prompted for password use the admin user password
sudo su -
3. edit the /etc/hosts file
vi /etc/hosts
4. insert a line below the last line for the FQDN of your source cluster. The syntax is:

Syntax: IP-Address Full-Qualified-Hostname Short-Hostname
Example: 172.16.89.45 sourcecluster.prod.superna.net source cluster

where
IP-Address is a node IP from the subnet pool where the source cluster FQDN is provisioned
Full-Qualified-Hostname is the FQDN that was used to add the Source cluster to Eyeglass

## Technical Advisory #11 - End of Support for 1.6.x Release Notice as of May 31, 2017

Effective July 30th, 2017 release 1.6.x, All customers running the above releases should upgrade to the latest release using upgrade guide located here. Numerous failover and performance improvements exist in the latest release with all new opened cases with this release will be asked to upgrade before issues are addressed as a first resolution step.

## Technical Advisory #12 - DR Dashboard/Zone Readiness display issue for Failed Over Status - no loss of failover functionality

Applies to Release 1.9, 1.9.1. The DR Dashboard Zone Readiness status may not show the Failed Over status for the Cluster which is currently inactive. This does not affect the ability to failover from the active cluster nor is it possible to initiate a failover from the inactive cluster.

Workaround: Policy Readiness and DFS Readiness correctly display the FAILED OVER Failover Status
To determine which cluster Eyeglass considers active:
1. Login the the Eyeglass web page.
2. Open the DR Dashboard.

3. Use the Policy Readiness or DFS Readiness view to determine which cluster is active for a specific policy.
4. Then the Zone Readiness vies can be used to confirm which Access Zone that policy falls under by opening the DR Failover Status window for an Access Zone and opening the OneFS SyncIQ Readiness folder. Here all of the SyncIQ Policies that are associated with Access Zone are listed.

This issue has been addressed in Release 1.9.2.

## Technical Advisory #13 - Spectra/Meltdown Available in Appliance 2.5.x

Upgrade path, follow this guide.

Note appliance defaults to weekly automatic critical patches and security updates if Internet connection is allowed to the appliance.
If you would like email notification of OS updates follow this link and register. http://lists.suse.com/mailman/listinfo/sle-security-updates.

The current Open SUSE status is explained here on this link https://www.suse.com/c/suse-addresses-meltdown-spectre-vulnerabilities/. The Open SUSE update will be posted to the mailing list once available.

CVE's below Available on appliances with 42.3 Open Suse

https://www.suse.com/security/cve/CVE-2017-5753/
https://www.suse.com/security/cve/CVE-2017-5715/

https://www.suse.com/security/cve/CVE-2017-5754/

## Technical Advisory #14 - EOS 1.9.x Releases

EOS for Releases 1.9.x March 20, 2018

## Technical Advisory #15 **- cross site scripting CVE on PowerScale**

cross site scripting vulnerabilities in CVE-2017-8024 requires a patch from PowerScale available for certain PowerScale release streams. This patch also requires disabling HTTP authentication which will affect Eyeglass directly. Eyeglass will not able to login to perform any DR functions. An updated version 2.5.3 will include alternate authentication solution for PowerScale to allow this complete CVE procedures to be applied. Partial implementation is possible by applying the path to PowerScale without disabling the HTTP authentication on the cluster

## Technical Advisory #16 **- Config Sync may skip steps on Error**

This issue is present in > 1.9.4 and can result in SMB shares and export not synced to DR if an object cannot be synced remaining objects are not attempted.

**Resolution:** Clear the error and all unsync changes will be synced successfully. A work around exists and requires a support case opened for instructions. This has been fixed in release 2.5.3 once it is GA. **We will also be releasing a patch to 2.5.2 that corrects this issue. The patch can be downloaded from the download page on located on the support site and will require download of the 2.5.2 offline installer and upgrading from 2.5.2 to latest build of 2.5.2 for an existing installation.**

## Technical Advisory #17 **- PowerScale CSRF Authentication is not compatible with Smartconnect and API services Affects Eyeglass releases 2.5.3 and later**

### NOTE: Only 2.5.3 and later supports a cluster with CSRF enabled.

**Issue**: PowerScale does NOT support multi node cluster aware CSRF sessions for authentication and is NOT compatible with Smartconnect FQDN method #1. This is known limitation of PowerScale CSRF implementation.

**Impact**: None. SSIP is fully supported with many deployments using this method. The load balancing of FQDN has some potential to expose issues on various nodes in the cluster and a minor performance improvement for large object customers.

**Resolution**: To support **CSRF** on PowerScale requires settings that disable basic HTTPS authentication and uses session tokens for authentication. This requires Eyeglass to use the SSIP in the management access zone due to above **PowerScale limitation**.

1. If you have added clusters to Eyeglass with FQDN (How to check: Open Inventory Icon, right click the cluster and select Edit to determine how Eyeglass was added).
2. Open Jobs icon, record all policy states in all sections of this window. You will need to re-enable these policies and enable DFS mode based on your records from this step.
3. Delete the cluster (right click menu on the cluster name, chose the delete option)
    a. Repeat the delete for each cluster listed in the inventory icon
    b. Re-add the cluster with the SSIP in the system access zone, enter eyeglass service account name used before and password
    c. Repeat for each cluster Note: more than one cluster can be added before submitting the inventory job
    d. Open Jobs Icon, then running jobs tab, wait for initial inventory to complete
    e. Once complete click on job definition tab and enable all jobs based on the recorded configurations from the step above.
    f. You may also need to enable DFS mode (How to enable DFS mode
    g. Use the bulk actions menu to enable the jobs (How to enable jobs)
    h. Then wait 5 minutes and verify all jobs are green
    i. If any errors, please open a support case.

# Technical Advisory #18 - **Ransomware Defender ECA cluster without Internet access potential for false positives**

**Issue**: In release 2.5.3 of Ransomware Defender a threat detector will sometimes match files that should not be considered Ransomware only when the ECA cluster does not have Internet access.

**Impact**: False positive detection of some users depending on the IO pattern.

**Resolution**: A new build of 2.5.3 with number 18257 is available for download now that addresses this issue, without any requirement to connect ECA clusters to the Internet.

1. Instructions to apply patch
2. Open a support case and request assistance to apply the patch.

## Technical Advisory #19 - SMB Data Integrity corner case can leave Deny permission on some or all shares

**Issue:** Normal configuration sync runs every 5 minutes and under some conditions may detect the Deny everyone permission used by the Data Integrity DR Assistant failover feature and sync it to the DR cluster before the deny is removed by the failover process. This is a corner case that has rare.

**Impact:** After a failover some SMB shares may be left with a deny everyone permission blocking access to users.

**Solution:** Manually remove the Deny Everyone permission on the affected shares.

**Solution to Use SMB Data Integrity Feature:**

1. Disable the config Sync Job before the failover
    a. using SSH to the Eyeglass appliance run:
    b. igls admin schedules set --id Replication --enabled false
2. After the failover is complete
    a. igls admin schedules set --id Replication --enabled true

**Resolution**: A new build of 2.5.4 with number 18275 has been released to address this issue.

## Technical Advisory #20 - PowerScale Auditing incorrectly records audit events for paths that do not exist on the cluster when SMB share is mounted with subfolders with a case that does not match the file system

Issue: Mounting below the SMB share of a file system path of **\ifs\data\temp** and the mount example \\dnsname\sharename\TEMP where temp is a subfolder will be audited incorrectly and recoreded as an audit event that does not exist in the file system. The audit event will be incorrectly created as /ifs/data/TEMP even though this path does not exist in the file system. PowerScale file system is case

senstive. **NOTE: If all SMB share mounts mount the share only and does not include subfolders this issue will not be seen, or if the subfolders of the mount matches the case of the actual file system.**

**NOTE: Onefs is a case senstive file system, NFS does not have this issue and denies mounts if the case does not match the actual file system case.**

**NOTE: Mounting the SMB share only, will allow Windows OS to auto correct the case when browsing the file system with explorer or command prompt and will not have this issue.**

**Best Practise:** If sub share mounts are needed , the case should match the file system path.

**Work Around:** With Easy Auditor start searches from the share path, not the sub path, only if you know you have mismatched mounts with sub folders.

**PowerScale fix for this bug**: No known fix planned

## Technical Advisory #21 - OneFS CLI command bug fails to exit ram

**Description of issue:** Onefs CLI command with a bug fails to exit after execution in some scenarios, The conditions for this to occur are unknown at this time.

A Onefs CLI command isi status has a bug that can cause the command to fail to exit memory. A patch exists from PowerScale support for this bug. This command is used by Eyeglass to collect

node usage data and runs on a schedule.  Due to this bug it is possible that this command may not exit ram and each new execution of the command will consume more ram on PowerScale nodes.

As a proactive measure the following steps should be followed to avoid the potential of ram usage consumption due to the Onefs CLI bug.

**Impact To Eyeglass DR:**  No impact by following these steps, no loss of DR functionality.

**Side Effects:**  An alarm may be raised about CLI data incomplete which can be ignored.

**Steps to follow:**

Remove these lines from your sudoer file or place a # at the front of the line and save it.

1. SSh to PowerScale
2. Edit the sudoer file using the PowerScale isi_visudo command.
3. Sudo file opens in vi editor.  place # in front of these lines
4. Save the file with :wq
5. eyeglass ALL=(ALL) NOPASSWD: /usr/bin/isi_for_array isi status*
6. eyeglass ALL=(ALL) NOPASSWD: /usr/bin/isi status*

# Technical Advisory #22 - Onefs 8.2 Does not support REST API or SSH SSIP connections from Eyeglass

1. Onefs releases 8.2 and later no longer support API connections or SSH connections needed by Eyeglass.  If you are planning an upgrade to 8.2 the following steps should be completed before your Onefs Upgrade to 8.2.
    a. Upgrade to 2.5.5 latest release number - Upgrade guide.
    b. Change the ip address used to add the cluster to Eyeglass to use a node IP in a system zone pool.  The pool should

be dynamic mode to ensure the IP will failover to other nodes.

c. This is done with the Inventory Icon, right click , edit , change the ip address, re-enter password and save.

d. Verify by opening the jobs icon and selecting a job with a check box, bulk actions , run now.  Then monitor in the running jobs icon.

e. For more detailed steps open a support case with support to assist or provide health check after the change has been made.

## Technical Advisory #23 - 2.5.6 Patch 1 Addresses failover Scenario's that can delay some steps from starting immediately

1. Some scenario's can cause delays in failover jobs starting to execute steps due to timeouts. An updated 2.5.6 patch addresses this issue.
2. **Recommendation**:  Upgrade to patch one following the offline upgrade steps here or open a support case for assistance.
3. Full release notes on patch 1 that includes additional fixes is available here

## Technical Advisory #24 Config Only Migration Job deletes shares and exports on the Destination Access Zone

In 2.5.6 build 84 or earlier this feature is a mirror mode and will remove any overlapping or non matching configuration data found on the target path or below. This will be changed in a patch release to default to merge mode and will leave all target configuration data as is and copy only new configuration to the target path. Note that a config only migration job will run on regular configuration replication cycle and if you are in this situation it should be deleted as it will delete any share or export you recreated to solve this problem on the next run.

## Technical Advisory #25 OneFS fails to create Quotas with corrupt configuration

During failover Quotas with corrupt / invalid configuration on the failover source cluster will be blocked from being created on the target cluster by OneFS. In the Superna Eyeglass failover log this will display as a quota error. For example a Quota on the source cluster with both Advisory and Advisory Threshold percentage configuration will be blocked by OneFS from being created on the target cluster with the message that only on advisory threshold option is supported. It is unknown how a Quota would enter this state on the source cluster and

Dell EMC should be contacted for troubleshooting/resolution of the corrupt quota configuration issue.

# Technical Advisory #26 Eyeglass VM Log4j Hardening

Eyeglass DR Edition Release with patched log4j version (click the About Eyeglass Icon to check your version)

1. 2.5.8 build **21330** - Only this exact build number includes the log4j 2.17, all other version can use the remediation steps below.

**Please Read below Exposure Statement:**

**Nessus Scanner using the profile below scanning the following releases returns no exposure to the log4J. This means the exploit would not succeed based on the scan results that attempts to use the exploit on all open IP ports. The Eyeglass vm does not expose ports that can be used to exploit this log4j CVE using a port scan and attack attempt.**

1. Eyeglass VM 2.5.7.1 and 2.5.8 releases - with no modifications made to these versions - **Passes a scan of the VM for the vulnerability**

This plugin is used in the scan template 'Log4Shell Vulnerability Ecosystem' as a way to include other plugins related to the Log4j vulnerabilities CVE-2021-44228 and CVE-2021-45046.
- 155998 Apache Log4j Message Lookup Substitution RCE (Log4Shell) (Direct Check)
- 155999 Apache Log4j < 2.15.0 Remote Code Execution
- 156000 Apache Log4j Installed (Unix)
- 156001 Apache Log4j JAR Detection (Windows)
- 156002 Apache Log4j < 2.15.0 Remote Code Execution
- 156014 Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP)
- 156017 SIP Script Remote Command Execution via log4shell
- 156016 Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP)
- 156035 VMware vCenter Log4Shell Direct Check (CVE-2021-44228) (VMSA-2021-0028)
- 156032 Log4j EOL / Unsupported Apache Log4j Unsupported Version Detection
- 156056 Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check)
- 156057 Apache Log4j 2.x < 2.16.0 DoS

**If you want to apply remediation to these product versions you can follow these steps below, read statement above.**

To remove the CVE present in log4j the following steps can be done.

1. Login to eyeglass
2. sudo -s

3. Run this command
    a. find /opt/superna -name '*.jar' | xargs -I {} zip -q -d {} org/apache/logging/log4j/core/lookup/JndiLookup.class
    b. **CVE-2021-4104**
        i. find /opt/superna -name '*.jar' | xargs -I {} zip -q -d {} org/apache/log4j/net/JMSAppender.class
4. Run the command a 2nd time
    a. find /opt/superna -name '*.jar' | xargs -I {} zip -q -d {} org/apache/logging/log4j/core/lookup/JndiLookup.class
    b. CVE-2021-4104
        i. find /opt/superna -name '*.jar' | xargs -I {} zip -q -d {} org/apache/log4j/net/JMSAppender.class
    c. If on the second execution all of the output states **"zip error: Nothing to do!" this means the patch was applied.**
5. Then run this command
    a. systemctl restart sca
6. done.

# Technical Advisory #27 - ECA VM Log4j Hardening - (Ransomware Defender, Easy Auditor, Performance Auditor)

Eyeglass ECA VM's patched log4j version (click the About Eyeglass Icon to check your version and the managed services icon to see the ECA version)

1. 2.5.8 build **21330** - Only this exact build number includes the log4j 2.17, all other version can use the remediation steps below.

These products use docker containers and isolate code in containers with minimal OS inside the container. The containers are ephemeral and are destroyed when the shut down commands are run. The steps below provide a method to disable the java class inside the containers that is part of the log4j CVE. The ECA VM's only communicate with the eyeglass VM and a firewall blocks all access to the VM's unless it originates from the eyeglass VM (release 2.5.7 and later). The steps below adds additional hardening to the ECA VM's recommended for all customers.

**Please Read below Exposure Statement:**

**Nessus Scanner using the profile below scanning the following releases returns no exposure to the log4J. This means the exploit would not succeed based on the scan results that attempts to use the exploit on all open IP ports. The ECA does not expose ports that can be used to exploit this log4j CVE.**

1. ECA (Ransomware Defender, Easy Auditor , Performance Auditor) 2.5.7.x releases - no modifications made to this version - **Pass**
2. ECA 2.5.8 - has updated log4j - **Pass**

This plugin is used in the scan template 'Log4Shell Vulnerability Ecosystem' as a way to include other plugins related to the Log4j vulnerabilities CVE-2021-44228 and CVE-2021-45046.
- 155998 Apache Log4j Message Lookup Substitution RCE (Log4Shell) (Direct Check)
- 155999 Apache Log4j < 2.15.0 Remote Code Execution
- 156000 Apache Log4j Installed (Unix)
- 156001 Apache Log4j JAR Detection (Windows)
- 156002 Apache Log4j < 2.15.0 Remote Code Execution
- 156014 Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP)
- 156017 SIP Script Remote Command Execution via log4shell
- 156016 Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP)
- 156035 VMware vCenter Log4Shell Direct Check (CVE-2021-44228) (VMSA-2021-0028)
- 156032 Log4j EOL / Unsupported Apache Log4j Unsupported Version Detection
- 156056 Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check)
- 156057 Apache Log4j 2.x < 2.16.0 DoS

**If you want to apply remediation to these product versions you can follow these steps below, read statement above.**

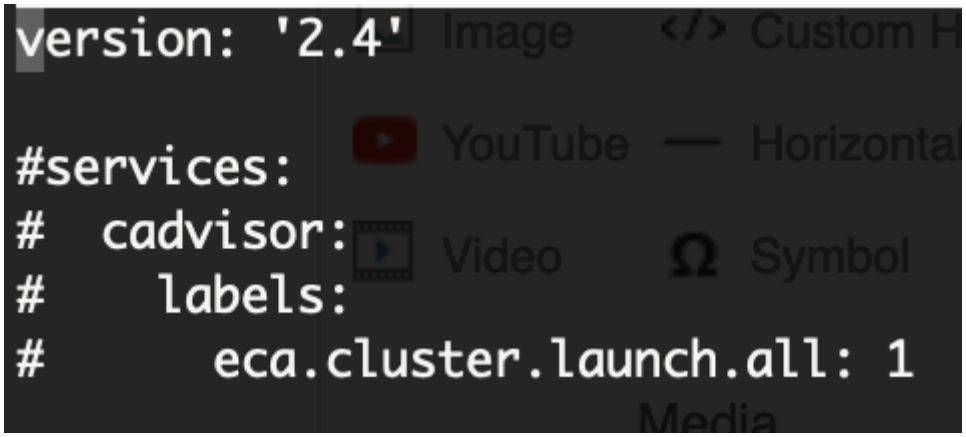
**Supported versions:**

1. 2.5.7 and 2.5.8
2. All other versions will need upgrade.

3. **NOTE: Make sure you have completed steps on technical advisory #26 above first on the eyeglass VM**

1. Login to ECA node 1 as ecaadmin user
2. Run this command to get the product version to determine which file to download
    a. ecactl version
    b. If 2.5.7 download this file (Right click the link and select "Save link as" option, to avoid your browser opening the file)
    c. if 2.5.8 download this file **(Right click the link and select "Save link as" option, to avoid your browser opening the file)**
3. Using winscp tool (https://winscp.net/eng/download.php)
    a. Login to node 1 of the eca vm **as the ecaadmin user** with winscp and copy the correct version of the file downloaded in step #2 to this path /opt/superna/eca
4. On the ssh login to eca node 1 **as the ecaadmin user**
    a. cat /opt/superna/eca/docker-compose.overrides.yml
    b. If your file looks like screenshot then continue to step #5, Only **if it does NOT look like below image**, open a case to get additional information on how to merge override files. **When opening the case attach the text of the docker-compose-overrides.yml file using output above.**

c.




5. Update the docker override file with the steps below.
    a. **2.5.8 release command (use the correct command for the release you are running)**
        i. cp /opt/superna/eca/docker-compose.CVE-2021-44228.2.5.8.yml  /opt/superna/eca/docker-compose.overrides.yml
    b. **2.5.7 release command** (use the correct command for the release you are running)
        i. cp /opt/superna/eca/docker-compose.CVE-2021-44228.2.5.7.yml /opt/superna/eca/docker-compose.overrides.yml
6. Restart the ECA cluster
    a. ecactl cluster down
    b. ecactl cluster exec 'sudo rm -rf /opt/superna/mnt/zk-ramdisk/*'
        i. **NOTE:  you will be asked to enter the ecaadmin password for each ECA VM to complete this command.**
    c. ecactl cluster up

    d. **Watch the cluster up log for any errors until it completes**
7. This will delete the docker containers and launch them all with the fix applied.
8. Verify with security guard and robo audit features normal operations
9. Done

## Technical Advisory #28 - Search & Recover, Golden Copy VM Log4j Hardening

These products use docker containers and isolate code in containers with minimal OS inside the container. The containers are ephemeral and are destroyed when the shut down commands are run. The steps below provide a method to disable the java class inside the containers that is part of the log4j CVE. The steps below adds additional hardening to the product VM's recommended for all customers.

**Please Read below Exposure Statement:**

**Nessus Scanner using the profile below scanning the following releases returns no exposure to the log4J. This means the exploit would not succeed based on the scan results that attempts to use the exploit on all open IP ports.**

1. Search & Recover 1.1.2, 1.1.5 release - no modifications made to this version - **Pass**

2. Golden Copy 1.1.6 no modifications made to this version - **Pass**

This plugin is used in the scan template 'Log4Shell Vulnerability Ecosystem' as a way to include other plugins related to the Log4j vulnerabilities CVE-2021-44228 and CVE-2021-45046.
- 155998 Apache Log4j Message Lookup Substitution RCE (Log4Shell) (Direct Check)
- 155999 Apache Log4j < 2.15.0 Remote Code Execution
- 156000 Apache Log4j Installed (Unix)
- 156001 Apache Log4j JAR Detection (Windows)
- 156002 Apache Log4j < 2.15.0 Remote Code Execution
- 156014 Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP)
- 156017 SIP Script Remote Command Execution via log4shell
- 156016 Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP)
- 156035 VMware vCenter Log4Shell Direct Check (CVE-2021-44228) (VMSA-2021-0028)
- 156032 Log4j EOL / Unsupported Apache Log4j Unsupported Version Detection
- 156056 Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check)
- 156057 Apache Log4j 2.x < 2.16.0 DoS

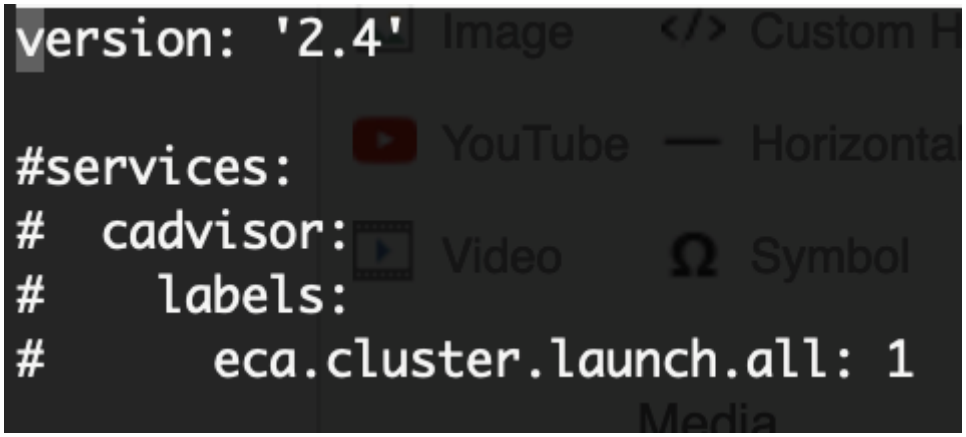
**If you want to apply remediation to these product versions you can follow these steps below, read statement above.**

**Supported versions:**

1. **Search & Recover release 1.1.5**
2. **Golden Copy releases 1.1.6**

1. Login to ECA node 1 as ecaadmin user
2. Run this command to get the product version to determine which file to download
    a. ecactl version
    b. Search & Recover
        i. If 1.1.2 download this file (Right click the link and select "Save link as" option, to avoid your browser opening the file)
        ii. if 1.1.5 download this file **(Right click the link and select "Save link as" option, to avoid your browser opening the file)**
    c. Golden Copy
        i. if 1.1.4 or 1.1.6 download this file (Right click the link and select "Save link as" option, to avoid your browser opening the file)
3. Using winscp tool (https://winscp.net/eng/download.php)
    a. Login to node 1 of the eca vm **as the ecaadmin user** with winscp and copy the correct version of the file downloaded in step #2 to this path /opt/superna/eca
4. On the ssh login to eca node 1 **as the ecaadmin user**
    a. **cat /opt/superna/eca/docker-compose.overrides.yml**
    b. If your file looks like screenshot then continue to step #5, Only **if it does NOT look like below image**, open a case to

get additional information on how to merge override files. **When opening the case attach the TEXT of the docker-compose-overrides.yml file using output above.**

c. 


5. Update the docker override file with the steps below.
    a. **Search & Recover 1.1.2 release command (use the correct command for the release you are running)**
        i. cp /opt/superna/eca/docker-compose.CVE-2021-44228.1.1.2.yml  /opt/superna/eca/docker-compose.overrides.yml
    b. **Search & Recover 1.1.5 release command** (use the correct command for the release you are running)
        i. cp /opt/superna/eca/docker-compose.CVE-2021-44228.1.1.5.yml /opt/superna/eca/docker-compose.overrides.yml
    c. **Golden Copy 1.1.4, or 1.1.6 release command** (use the correct command for the release you are running)
        i. cp /opt/superna/eca/docker-compose.CVE-2021-44228.gc.yml /opt/superna/eca/docker-compose.overrides.yml

6. Update configuration file ONLY for Search & Recover (both versions)
    a. nano /opt/superna/eca/eca-env-common.conf
    b. add this line to the file (location in the file  does not matter) copy and paste.
    c. **export SOLR_JAVA_OPTS="-XX:MaxDirectMemorySize=8g -DformatMsgNoLookups=true"**
    d. save the file with control+x  (answer yes to save the file)
7. Restart the product cluster (Applies to Search & Recover and Golden Copy)d
    a. ecactl cluster down
    b. ecactl cluster up
    c. **Watch the cluster up log for any errors until it completes**
8. This will delete the docker containers and launch them all with the fix applied.
9. Verify Search & Recover by logging into the gui and run a search
10. Verify Golden Copy by running a copy command or login to the GUI
11. Done

# Technical Advisory #29 CVE-2021-45046 log4j (2.16) - Does not apply to any Superna product

This CVE-2021-45046 (**log4j 2.16**) does not apply to any Superna products. **This vulnerability does not apply since the MDC function is not used and this CVE requires that function to be used to be exposed.**

**Nessus Scanner using this profile all pass 2.5.7.x with remediation applied and 2.5.8 with CVE patch all pass scans with no vulnerability.**

This plugin is used in the scan template 'Log4Shell Vulnerability Ecosystem' as a way to include other plugins related to the Log4j vulnerabilities CVE-2021-44228 and CVE-2021-45046, including those based on patches from other vendors.
- 155998 Apache Log4j Message Lookup Substitution RCE (Log4Shell) (Direct Check)
- 155999 Apache Log4j < 2.15.0 Remote Code Execution
- 156000 Apache Log4j Installed (Unix)
- 156001 Apache Log4j JAR Detection (Windows)
- 156002 Apache Log4j < 2.15.0 Remote Code Execution
- 156014 Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP)
- 156017 SIP Script Remote Command Execution via log4shell
- 156016 Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP)
- 156035 VMware vCenter Log4Shell Direct Check (CVE-2021-44228) (VMSA-2021-0028)
- 156032 Log4j EOL / Unsupported Apache Log4j Unsupported Version Detection
- 156056 Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check)

- 156057 Apache Log4j 2.x < 2.16.0 DoS

# Technical Advisory #30 How to Mitigate Vulnerabilities in JRE 1.8.0_291 in Eyeglass Appliance

These opensuse vulnerabilities exist in the embedded Java JRE

Applies to 2.5.7.x and 2.5.8.0 and 2.5.8.1

1. https://www.tenable.com/plugins/nessus/154345 CVE-2021-3517
    a. Login as admin
    b. sudo -s
    c. mv /opt/superna/java/jre/lib/ext/jfxrt.jar /opt/superna/java/jre/lib/ext/jfxrt.bak
    d. systemctl restart sca
2. Does not apply to Eyeglass (This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator)
    a. https://www.tenable.com/plugins/nessus/154345
    b. https://www.tenable.com/plugins/nessus/152021
    c. https://www.tenable.com/plugins/nessus/148961

# Technical Advisory #31 Ransomware Defender NFS Event Detection Always Enabled in 2.5.8.1-22080/22100

In Ransomware Defender 2.5.8.1-22080 and 2.5.8.1-22100, NFS Event Detection is always enabled and cannot be turned off. For environments with NFS workload, even if NFS Event Detection was not previously enabled this can lead to new detections and possible unexpected lockout for NFS events if Ransomware Defender is in Enforcement mode.

**NOTE: if you use only SMB, this advisory does NOT apply to you, you can still make the change below.**

**NOTE: If you are in monitor mode, no impact but the change below should be applied.**

Workaround:

1. Login to node 1 of the eca cluster as ecaadmin
2. ecactl cluster down
3. nano /opt/superna/eca/eca-env-common.conf
4. add this variable
5. export TURBOAUDIT_PROTCOL_FILTER_ENABLD=true
6. Save and exit with control+x (answer yes)
7. ecactl cluster up

8. Done.  The NFS lockout will be disabled.