CONTINUITY

StorageGuard

Risk Assessment Summary Report

Data Storage Systems: Security Configuration Analysis

Prepared for: XYZ Bank

Issued by: Continuity

November 2021

Table of Content

Introduction

XYZ Bank invited **Continuity** to perform a data storage security risk assessment on a subset of its production environment to identify data system security misconfigurations and vulnerabilities.

Continuity's **StorageGuard™** collects and analyzes configuration data from all enterprise storage and hardware systems. A built-in risk detection engine checks for thousands of possible misconfigurations and vulnerabilities at the storage system level that pose a security threat to your critical business data. This includes analyzing the configuration of block, object and IP storage systems, Cloud storage, SAN / NAS, storage management servers, storage appliances, virtual SAN, FCoE / iSCSI / FC, File systems, storage network switches, data protection appliances, storage virtualization systems and other storage devices. **SG** identifies violations of vendor security configuration guidelines, organizational security baseline requirements (built-in and custom), community-driven best practices, compliance requirements (CIS, NIST, PCI DSS and more) and vulnerabilities. The **SG** Risk Signature Knowledgebase™ includes built-in automatic checks for authentication configuration, administrative access, storage access control, insecure protocols and services, ransomware protection guidelines, file shares security recommendations, NIST SP800-53 requirements, storage CVEs and more. Remediation of such risks will harden the data storage environment and protect critical business data from attacks.

When a risk is discovered by **SG**, a detailed description and the suggested resolution are forwarded to the right IT teams for timely action. **SG** operation is agentless, secure, and non-intrusive.

Such risks are the natural result of a large volume of ongoing changes within a highly complex technology environment. Given the nature of such environments, it is practically impossible to manually identify such issues. Automated, proactive discovery of these irregularities is critical to preventing data security risks and successfully completing Information Security audits.

Executive Summary

Overview

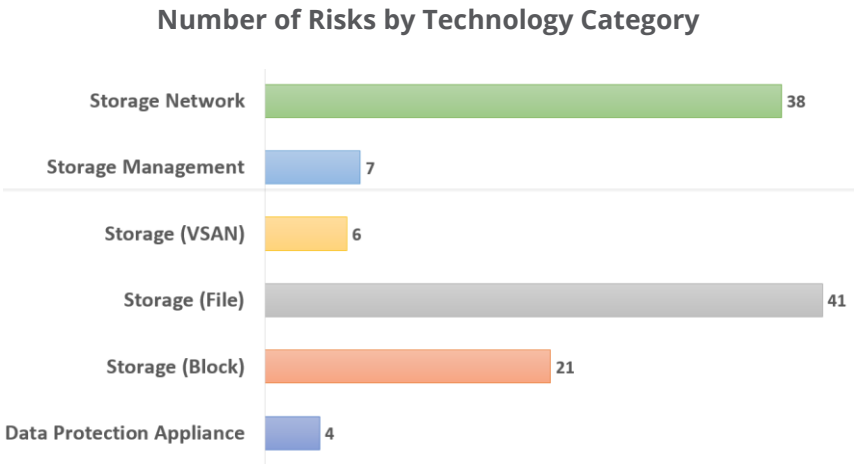
- A subset of the production environment was scanned and analyzed by **SG**.
- The one-time collection of configuration data was performed using **SG'**s agentless scan technology, with no impact on production and without installing any software on the target systems.
- The following systems were included in the scan scope:
    - The data systems used by **Payments**, **CRM** and **Billing** applications
    - Storage systems (block, file, object and cloud)
    - Storage virtualization and data protection appliances
    - Storage network
- See Risk Assessment Scope for a detailed scope list

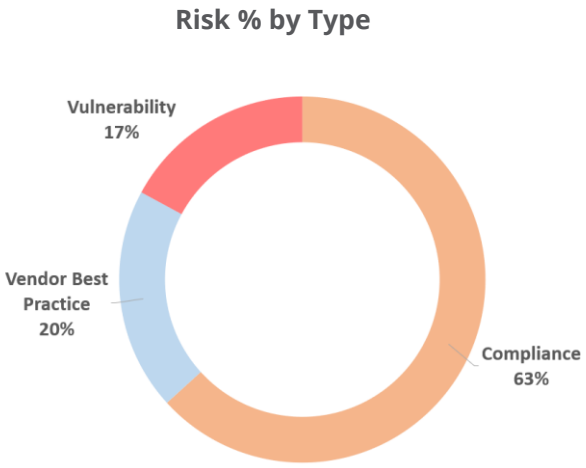
Risk Assessment Findings

- A total of **28 risk types** were detected, consisting of **117 individual risks**.
- See Summary of Risk Types.
- The data security vulnerability and compliance risks identified span all layers of the storage infrastructure, including **file and block storage, virtual SAN, storage network, storage management systems** and more**.**
- A detailed, prioritized listing of all 117 issues found is included in this report. See Index of Individual Risks – Prioritized.

Conclusions

- Significant **data security risks identified for data systems used by Payments, Billing and CRM.**
- Detailed information is available through this report for the compliance risks, vulnerabilities and security best practice violations identified by **SG**. See Analysis of Findings.
- It is practically impossible to manually identify such risks - though simple to repair once found.
- Similar and other issues may be present in the un-scanned portion of the production environment.
- Running a daily scan on all critical systems at XYZ Bank is highly recommended.
- This report details the risks identified and includes the corrective steps required for remediation.





Risk Assessment Scope

Target System	Detected	Scanned	% of non-compliance
Block Storage			
EMC VMAX	9	9	66%
HP 3PAR	14	14	50%
Hitachi VSP G1000	6	5	34%
EMC VNX	19	18	47%
Object Storage			
Hitachi Content Platform	3	3	0%
File Storage			
NetApp	24	24	45%
EMC Isilon	9	9	22%
EMC Data Domain	2	2	100%
Cloud Storage			
Amazon S3	1	1	0%
Virtual SAN			
EMC ScaleIO	10	10	60%
Storage Appliance			
EMC RecoverPoint	2	2	100%
IBM SVC	2	2	0%
Storage Network			
Cisco MDS Switch	24	23	48%
Brocade FC Switch	31	29	16%
Cisco UCS Switch	16	15	4%
HP FlexFabric Switch	8	8	0%

Summary of Risk Types

A total of **28 risk types** were detected, consisting of 117 individual risks.

The risk types are listed below. For the individual risks, see Index of Individual Risks – Prioritized.

System Type	Risk Name	Category	Risk Type	Risk Count
Hitachi G1000	HDS Arbitrary Command Execution Vulnerability	Storage Management	Vulnerability	2
Cisco MDS	Unsecure Protocols Enabled	Storage Network	Vendor Best Practice	6
HP 3PAR	Local User Account Control	Storage (Block)	Compliance	7
Brocade FC	Unsecure Zone Member Identification	Storage Network	Vendor Best Practice	4
Brocade FC	Local User Account Control	Storage Network	Compliance	1
EMC ScaleIO	ScaleIO Buffer Overflow Vulnerability	Storage (VSAN)	Vulnerability	6
Brocade FC	No Authentication for SNMP	Storage Network	Compliance	4
Cisco MDS	Local User Account Control	Storage Network	Compliance	2
Cisco MDS	Single Timekeeping Server	Storage Network	Vendor Best Practice	11
NetApp	ONTAP Authentication Bypass Vulnerability	Storage (File)	Vulnerability	3
NetApp	Unrestricted NFS Client IP Addr	Storage (File)	Compliance	5
Cisco MDS	Timekeeping not configured	Storage Network	Vendor Best Practice	2
Cisco MDS	Central Log Server not Configured	Storage Network	Compliance	5
NetApp	Unapproved Storage Software	Storage (File)	Compliance	4
Cisco MDS	No Authentication for SNMP	Storage Network	Compliance	3
EMC Isilon	OneFS Privilege Escalation Vulnerability	Storage (File)	Compliance	2
EMC Data Domain	Local User Account Control	Storage (File)	Compliance	1
EMC VMAX	EMC VAPP Authentication Bypass Vulnerability	Storage Management	Vulnerability	5
EMC Data Domain	Central Log Server not Configured	Storage (File)	Compliance	2
EMC Isilon	NFSv3/4 not Enabled	Storage (File)	Compliance	3
NetApp	Central Log Server not Configured	Storage (File)	Compliance	7
NetApp	Unsecure NetApp SNMP Community Settings	Storage (File)	Compliance	3
EMC RecoverPoint	RPA Command Injection Vulnerability	Data Protection Appliance	Vulnerability	4

NetApp	Unapproved Local Account	Storage (File)	Compliance	2
NetApp	Unrestricted NFS Access to root	Storage (File)	Compliance	6
NetApp	Ransomware protection not enabled	Storage (File)	Compliance	3
EMC VNX	Unapproved Storage Software	Storage (Block)	Compliance	5
EMC VNX	Local User Account Control	Storage (Block)	Compliance	9
			Total	**117**

Index of Individual Risks - Prioritized

The following table lists all the risks identified, sorted by the priority ("Rating") assigned by a Continuity engineer, after a thorough examination of each risk.

*This Example Report shows one risk per each risk type

ID	Summary	Rating	Risk Type
142	Cisco switch **CIS-SW-ROC-60** at site **Rochester** has unsecure protocols enabled.		Unsecure Protocols Enabled
293	HP 3PAR **TQDC3PAR0001** at site **Tokyo** has local users with unlimited rights that are not controlled through an account vault solution.		Local User Account Control
543	Zones of Brocade switch **DCX8510-LN-BK01** at site **London** are defined with unrecommended Domain,Port (D,P) identification.		Unsecure Zone Member Identification
354	Hitachi storage management server **192.2.0.56** at site **Austin** is exposed to an arbitrary command execution vulnerability.		HDS Arbitrary Command Execution Vulnerability
611	Brocade switch **sanswc45** at site **Tokyo** has un-vaulted local accounts.		Local User Account Control
681	ScaleIO storage server **sio034** at site **Rochester** is exposed to a buffer overflow vulnerability.		ScaleIO Buffer Overflow Vulnerability
755	Brocade switch **DCX85-SAN-AUS-01** at site **Austin** is configured with noAuth for SNMP.		No Authentication for SNMP
71	Cisco switch **CIS-SW-ROC-8** at site **Rochester** has un-vaulted local accounts.		Local User Account Control
196	Cisco switch **CIS-SW-LON-43** at site **London** is configured with only one NTP server.		Single Timekeeping Server
603	NetApp filer **nasprd12** at site **Austin** is exposed to an authentication bypass vulnerability.		ONTAP Authentication Bypass Vulnerability
282	NetApp cluster **tlddr1010** at site **Rochester** has policies with unrestricted client IP range.		Unrestricted NFS Client IP Addr
125	Cisco switch **CIS-A-TOK-23** at site **Tokyo** has no timekeeping servers configured.		Timekeeping not configured
84	Cisco switch **C3-SW-A-98** at site **Austin** is not configured with a Logging server.		Central Log Server not Configured
1002	NetApp cluster **tlddr1011** at site **Rochester** is installed with unapproved software.		Unapproved Storage Software
342	Cisco switch **CIS-SW-AUS-B-19** at site **Austin** is configured with noAuth for SNMP.		No Authentication for SNMP
195	EMC Isilon **isdatap23** at site **Rochester** is exposed to a privilege escalation vulnerability.		OneFS Privilege Escalation Vulnerability
315	Data Domain **APM00139404415** at site **London** has un-vaulted local accounts.		Local User Account Control

715	EMC vApp **univmax** at site **Austin** is exposed to an authentication bypass vulnerability.		EMC VAPP Authentication Bypass Vulnerability
7	EMC Data Domain **APM00139404415** at site **London** is not enabled with remote logging.		Central Log Server not Configured
360	EMC Isilon **isdatalo55** at site **Tokyo** is not enabled with NFSv3/4.		NFSv3/4 not Enabled
645	NetApp filer **pdocut2file** at site **Austin** is not configured with a central log server.		Central Log Server not Configured
627	NetApp filer **nasprd101** at site **Austin** is configured with unsecure SNMP community settings.		Unsecure NetApp SNMP Community Settings
351	RecoverPoint **192.23.1.42** at site **London** is exposed to a command injection vulnerability.		RPA Command Injection Vulnerability
81	NetApp cluster **tlddr1010** at site **Rochester** has unauthorized local user accounts.		Unapproved Local Account
223	NetApp cluster **ausddr023** at site **Rochester** has unrecommended anonymous user NFS settings.		Unrestricted NFS Access to root
283	NetApp cluster **tlddr1010** at site **Rochester** is not enabled with ransomware protection features.		Ransomware Protection not Enabled
1210	EMC VNX **SYSVNX0011** at site **London** is installed with unapproved software.		Unapproved Storage Software
1273	EMC VNX **EUR0-VNX0500** at site **London** has un-vaulted local user accounts.		Local User Account Control

Risk 142

Risk ID	I00082	Name	Unsecure Protocols Enabled
Severity	WARNING	Status	OPEN
Categories	Security Compliance		
Area	Storage Network		
Labels	Cisco, Protocols, Vendor Best Practice, Compliance, PCI DSS 2.3, CISv7 Control		

Summary

Cisco switch **CIS-SW-ROC-60** at site **Rochester** has unsecure protocols enabled.

Description

Cisco switch **CIS-SW-ROC-60** at site **Rochester** has enabled networking services that do not use encryption:

Service	Action setting
HTTP	enabled
Telnet	disabled

Impact

If non-console (including remote) administration does not use secure authentication and encrypted communications, sensitive administrative or operational level information (like administrator IDs and passwords) can be revealed to an eavesdropper. A malicious individual could use this information to access the network, become administrator, and steal data. Clear-text protocols (such as HTTP, telnet, etc.) do not encrypt traffic or logon details, making it easy for an eavesdropper to intercept this information. Clear text protocols are vulnerable to sniffing, interception and other attacks.

Resolution

Disable the use of Telnet and HTTP on the switch.

Risk 293

Risk ID	C00183	Name	Local User Account Control
Severity	ERROR	Status	OPEN
Categories	Security Compliance		
Area	Storage (Block)		
Labels	3PAR, HPE, IAM, Compliance, NIST SP 800-53 IA-2, CISv7 Control 16.2, HIPAA 164.312(a)(1), COBIT 5 DSS05.04, PCI DSS 8.1, ISO/IEC 27001 A.9.2, NIST SP800-53 AC-2		

Summary

HP 3PAR **TQDC3PAR0001** at site **Tokyo** has local users with unlimited rights that are not controlled through an account vault solution.

Description

HP 3PAR **TQDC3PAR0001** at site **Tokyo** has local users with unlimited rights that are not controlled through an account vault solution. Authentication control does not meet the required standard.

The following table shows the users in violation:

User	Role	Default
lore	super	no
steve_old	super	no
admgrp1	super	no

Impact

Enforcement of required security policies such as password expiration and length are not available. Such users can potentially be used by attackers to gain unauthorized admin access to the storage system. Failing to meet this practice may lead to security audit failures and to increased risk of unauthorized access.

Resolution

Configure your organizational account vault solution to manage the identified local users.

Risk 543

Risk ID	I00682	Name	Unsecure Zone Member Identification
Severity	WARNING	Status	OPEN
Categories	Security Compliance		
Area	Storage Network		
Labels	Brocade, SAN Zoning, Storage Access Control, Vendor Best Practice, Community BP		

Summary

Zones of Brocade switch **DCX8510-LN-BK01** at site **London** are defined with unrecommended Domain, Port (D,P) identification.

Description

Zones of Brocade switch **DCX8510-LN-BK01** at site **London** are defined with Domain,Port (D,P) identification, in contrast to the Brocade security guidelines.

The following table shows the zones in violation:

FID	Zone	Member
128	zt1hds	1,2 1,10
128	zt1hds	1,2 1,10

Impact

Any device physically cabled to a port could inappropriately grant storage access. Risk of unauthorized hosts being cabled to the wrong switch port.

Resolution

Use **pWWN** identification only, remove Domain,Port (D,P) members.

Risk 354

Risk ID	V00371	Name	HDS Arbitrary Command Execution Vulnerability
Severity	ERROR	Status	OPEN
Categories	Security Vulnerability		
Area	Storage Management		
Labels	Hitachi, HDS, CVE		

Summary

Hitachi storage management server **192.2.0.56** at site **Austin** is exposed to an arbitrary command execution vulnerability.

Description

Hitachi storage management server **192.2.0.56** at site **Austin** is installed with the following vulnerable software:

- Hitachi Device Manager 8.4.1-02

Impact

An attacker can exploit this issue to execute arbitrary commands within the context of the vulnerable application. Refer to https://www.cvedetails.com/cve/CVE-2017-9294 for additional detail.

Resolution

Hitachi Device Manager 8.4.1-02 - Upgrade vulnerable software to version 8.5.2-01.

Risk 611

Risk ID	C00183	Name	Local User Account Control
Severity	WARNING	Status	OPEN
Categories	Security Compliance		
Area	Storage Network		
Labels	Brocade, IAM, Compliance, NIST SP 800-53 IA-2, CISv7 Control 16.2, HIPAA 164.312(a)(1), COBIT 5 DSS05.04, PCI DSS 8.1, ISO/IEC 27001 A.9.2, NIST SP800-53 AC-2		

Summary

Brocade switch **sanswc45** at site **Tokyo** has un-vaulted local user accounts.

Description

Brocade switch **sanswc45** at site **Tokyo** has local users with unlimited rights that are not controlled through an account vault solution. Authentication control does not meet the required standard.

Un-vaulted local user list:

- carladmin
- opsuser

Impact

Enforcement of required security policies such as password expiration and length are not available. Such users can potentially be used by attackers to gain unauthorized admin access to the storage system. Failing to meet this practice may lead to security audit failures and to increased risk of unauthorized access.

Resolution

Configure your organizational account vault solution to manage the identified local users or remove them.

Risk 681

Risk ID	V00199	Name	ScaleIO Buffer Overflow Vulnerability
Severity	ERROR	Status	OPEN
Categories	Security Vulnerability		
Area	Storage		
Labels	ScaleIO, Dell EMC, VSAN, CVE		

Summary

ScaleIO storage server **sio034** at site **Rochester** is exposed to a buffer overflow vulnerability.

Description

ScaleIO storage server **sio034** at site **Rochester** is installed with the following vulnerable software:

- EMC ScaleIO 2.0.1.2

Impact

Attackers can execute arbitrary code in the context of the affected application. Failed exploit attempts will result in a denial-of-service condition. Refer to https://www.cvedetails.com/cve/CVE-2017-8020 for additional detail.

Resolution

EMC ScaleIO 2.0.1.2 - Upgrade vulnerable software to version 2.0.1.4.

Risk 755

Risk ID	C00286	Name	No Authentication for SNMP
Severity	WARNING	Status	OPEN
Categories	Security Compliance		
Area	Storage Network		
Labels	Brocade, SAN, SNMP, Cisco Security Baseline, PCI DSS 8.2, ISO/IEC 27001 A.9.4.2, NIST SP800-53 IA-3		

Summary

Brocade switch **DCX85-SAN-AUS-01** at site **Austin** is configured with noAuth for SNMP.

Description

Brocade switch **DCX85-SAN-01** at site **Austin** has 5 local users that are set without an authentication requirement when using SNMPv3:

- admin
- tracyM
- snmpuser
- brcdadm

Impact

SNMPv3 implementations must be configured with the authPriv HMAC or authNoPriv HMAC security level. NoAuth, NoPriv must not be used. Failing to meet this practice may lead to security audit failures and to increased risk of unauthorized access.

Resolution

Set authentication as required when SNMPv3 is used.

Risk 71

Risk ID	C00183	Name	Local User Account Control
Severity	ERROR	Status	OPEN
Categories	Security Compliance		
Area	Storage Network		
Labels	Cisco, IAM, Compliance, NIST SP 800-53 IA-2, CISv7 Control 16.2, HIPAA 164.312(a)(1), COBIT 5 DSS05.04, PCI DSS 8.1, ISO/IEC 27001 A.9.2, NIST SP800-53 AC-2		

Summary

Cisco switch **CIS-SW-ROC-8** at site **Rochester** has un-vaulted local accounts.

Description

Cisco switch **CIS-SW-ROC-8** at site **Rochester** has local users with unlimited rights that are not controlled through an account vault solution:

- lenuser
- ciscogtw

Impact

Access to Fiber Channel switch must use a centralized authentication access method. In addition, Factory default local accounts must use a password vaulting solution. Failing to meet this practice may lead to security audit failures and to increased risk of unauthorized access.

Resolution

Configure your organizational account vault solution to manage the identified local users or remove them.

Risk 196

Risk ID	I00513	Name	Single Timekeeping Server
Severity	WARNING	Status	OPEN
Categories	Security Compliance		
Area	Storage Network		
Labels	Cisco, SAN, NTP, Time Synchronization, Timekeeping, Compliance, Vendor Best Practice, ISO/IEC 27001 A.12.4.4, PCI DSS 10.4, NIST SP800-53 AU-8, CISv7 Control 6.1		

Summary

Cisco switch **CIS-SW-LON-43** at site **London** is configured with only one NTP server.

Description

Cisco switch **CIS-SW-LON-43** at site **London** has only one NTP server defined:

- 166.42.101.86

Impact

Switches must synchronize the time with the NTP (Network Time Protocol) hierarchy for time-synchronization using a minimum of two time servers.

Resolution

Configure the switch to work with at least two NTP active servers.

Risk 603

Risk ID	V00021	Name	ONTAP Authentication Bypass Vulnerability
Severity	ERROR	Status	OPEN
Categories	Security Vulnerability		
Area	Storage (File)		
Labels	NetApp, CVE		

Summary

NetApp filer **nasprd12** at site **Austin** is exposed to an authentication bypass vulnerability.

Description

NetApp filer **nasprd12** at site **Austin** is installed with a vulnerable ONTAP release.

The following table lists the affected NetApp system and installed vulnerable version:

Storage System	Type	ONTAP release
nasprd12	NetApp (7-mode)	8.2.3

Impact

Remote attackers could obtain sensitive information and/or modify volumes via vectors related to UTF-8 in the volume language. Refer to https://nvd.nist.gov/vuln/detail/CVE-2015-7746 for additional detail.

Resolution

Remove UTF-8 from the volume language (unrecommended) or install required ONTAP software updates.

Risk 282

Risk ID	C00107	Name	Unrestricted NFS Client IP Addr
Severity	WARNING	Status	OPEN
Categories	Security Compliance		
Area	Storage (File)		
Labels	NetApp, Compliance, NAS, NFS, CISv7 Control 14.6, PCI DSS 7, HIPAA		

Summary

NetApp cluster **tlddr1010** at site **Rochester** has policies with unrestricted client IP range.

Description

Shares on NetApp cluster **tlddr1010** at site **Rochester** are not restricted to a specific IP or cluster.

The following table lists the affected vservers:

Vserver	Policy Name	Clientmatch
tlddr1010svm	default	0.0.0.0/0
tlddr1010svm	open	0.0.0.0/0

Impact

NFS exports must be specific to IP address/machine name/netgroup and not contain subnets or "all hosts". Failing to meet this practice may lead to security audit failures and to increased risk of unauthorized access.

Resolution

Restrict access to share drives to a single server or cluster.

Risk 125

Risk ID	I00510	Name	Timekeeping not configured
Severity	ERROR	Status	OPEN
Categories	Security Compliance		
Area	Storage Network		
Labels	Cisco, SAN, NTP, Time Synchronization, Timekeeping, Compliance, Vendor Best Practice, ISO/IEC 27001 A.12.4.4, PCI DSS 10.4, NIST SP800-53 AU-8, CISv7 Control 6.1		

Summary

Cisco switch **CIS-A-TOK-23** at site **Tokyo** has no timekeeping servers configured.

Description

Cisco switch **CIS-A-TOK-23** at site **Tokyo** has no NTP servers defined.

Impact

Switches must synchronize the time with the NTP (Network Time Protocol) hierarchy for time-synchronization using a minimum of two time servers.

When clocks are not properly synchronized, it can be difficult, if not impossible, to compare log files from different systems and establish an exact sequence of event (crucial for forensic analysis in the event of a breach). For post-incident forensics teams, the accuracy and consistency of time across all systems and the time of each activity is critical in determining how the systems were compromised.

Resolution

Set the switch to work with at least two NTP active servers.

Risk 84

Risk ID	C00727	Name	Central Log Server not Configured
Severity	WARNING	Status	OPEN
Categories	Security Compliance		
Area	Storage Network		
Labels	Cisco, SAN, Audit Logging, syslog, NIST SP800-53 AU-4.1, PCI DSS 10.5.4, PCI DSS 10.5.3, ISO/IEC 27001 A.16.1.7		

Summary

Cisco switch **C3-SW-A-98** at site **Austin** is not configured with a Logging server.

Description

The logging server definitions of Cisco switch **C3-SW-A-98** at site **Austin** logging server are misconfigured:

Logging server status	Logging server IP
disabled	N/A

Impact

All logs must be time-stamped and sent to approved central syslog repository. Failing to meet this practice may lead to security audit failures and to increased risk of unauthorized access.

Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible. Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs, and they do not know that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files. By writing logs to central log servers, the risk of those logs being lost or altered is lowered, as they are more secure within the internal network.

Off-loading is a process designed to preserve the confidentiality and integrity of audit records by moving the records from the primary information system to a secondary or alternate system. It is a common process in information systems with limited audit storage capacity; the audit storage is used only in a transitory fashion until the system can communicate with the secondary or alternate system designated for storing the audit records, at which point the information is transferred.

By writing logs to central and hardened log servers, the risk of those logs being lost or altered is lowered, as they are more secure within the internal network. Without central log servers, an organization may fail to meet audit log retention and accuracy requirements.

Resolution

Logging server must be enabled, and one or more servers or IP addresses must be listed.

Risk 1002

Risk ID	C00299	Name	Unapproved Storage Software
Severity	WARNING	Status	OPEN
Categories	Security Compliance		
Area	Storage (File)		
Labels	NetApp, NAS, SAN, Compliance, NIST SP800-53 SA-22, CISv7 Control 2.6		

Summary

NetApp cluster **tlddr1011** at site **Rochester** is installed with unapproved software.

Description

NetApp cluster **tlddr1011** at site **Rochester** is installed with unapproved code. The installed version is not listed in the *ApprovedVersions.xml* file.

The following table lists the affected systems:

Array name	Model	Version	Software status	Code level
tlddr1011n1	AFF8080	9.1P14	N/A	N/A
tlddr1011n2	AFF8080	9.1P14	N/A	N/A

Impact

Storage systems and their underlying components must be built and updated with the latest certified code with associated security updates, patches and service packs, including remediation of all GIS vulnerability assessment findings.

Resolution

Update the array software version to the approved software code.

Risk 342

Risk ID	C00286	Name	No Authentication for SNMP
Severity	ERROR	Status	OPEN
Categories	Security Compliance		
Area	Storage Network		
Labels	Cisco, SAN, SNMP, Cisco Security Baseline, PCI DSS 8.2, ISO/IEC 27001 A.9.4.2, NIST SP800-53 IA-3		

Summary

Cisco switch **CIS-SW-AUS-B-19** at site **Austin** is configured with noAuth for SNMP.

Description

Cisco switch **CIS-SW-AUS-B-19** at site **Austin** has 2 local users that are set without an authentication requirement when using SNMPv3:

- kimadm
- fcsuper

Impact

Authentication is required when SNMPv3 is used. SNMPv3 implementations must be configured with the authPriv HMAC or authNoPriv HMAC security level. NoAuth, NoPriv must not be used. Failing to meet this practice may lead to security audit failures and to increased risk of unauthorized access.

Resolution

Set authentication as required when SNMPv3 is used.

Risk 195

Risk ID	V00043	Name	OneFS Privilege Escalation Vulnerability
Severity	ERROR	Status	OPEN
Categories	Security Vulnerability		
Area	Storage (File)		
Labels	Isilon, OneFS, CVE		

Summary

EMC Isilon **isdatap23** at site **Rochester** is exposed to a privilege escalation vulnerability.

Description

EMC Isilon **isdatap23** at site **Rochester** is installed with a vulnerable OneFS release.

The following table lists the storage systems in violation:

Storage System	Type	OneFS Version
isdatap23	EMC Isilon	8.1.0.0

Impact

Remote attackers could potentially access and corrupt data of multiple applications. Refer to https://www.cvedetails.com/cve/CVE-2017-4988 for additional detail.

Resolution

Upgrade to a non-vulnerable OneFS version or install required patches.

Risk 315

Risk ID	C00183	Name	Local User Account Control
Severity	WARNING	Status	OPEN
Categories	Security Compliance		
Area	Storage (File)		
Labels	Data Domain, IAM, Compliance, NIST SP 800-53 IA-2, CISv7 Control 16.2, HIPAA 164.312(a)(1), COBIT 5 DSS05.04, PCI DSS 8.1, ISO/IEC 27001 A.9.2, NIST SP800-53 AC-2		

Summary

Data Domain **APM00139404415** at site **London** has un-vaulted local accounts.

Description

Data Domain **APM00139404415** at site **London** has local users with unlimited rights that are not controlled through an account vault solution:

- bckusr1
- stomaster

Impact

Access to Fiber Channel switch must use a centralized authentication access method. In addition, Factory default local accounts must use a password vaulting solution. Failing to meet this practice may lead to security audit failures and to increased risk of unauthorized access.

Resolution

Remove un-vaulted local accounts from the switch.

Risk 715

Risk ID	V00174	Name	EMC VAPP Authentication Bypass Vulnerability
Severity	ERROR	Status	OPEN
Categories	Security Vulnerability		
Area	Storage Management		
Labels	EMC, VMAX, Unisphere, CVE		

Summary

EMC vApp **univmax** at site **Austin** is exposed to an authentication bypass vulnerability.

Description

EMC vApp **univmax** at site **Austin** is installed with a vulnerable EMC Unisphere for VMAX Virtual Appliance release.

The following table lists the storage management systems in violation:

Storage Management System	Type	Version
Univmax	• EMC Unisphere for VMAX Virtual Appliance • Solutions Enabler	8.2

Impact

An attacker can exploit this issue to bypass authentication mechanism and perform unauthorized actions. This may lead to further attacks. Refer to https://www.cvedetails.com/cve/CVE-2016-6645 for additional detail.

Resolution

Upgrade to a non-vulnerable EMC vApp version or install required patches.

Risk 7

Risk ID	C00727	Name	Central Log Server not Configured
Severity	WARNING	Status	OPEN
Categories	Security Compliance		
Area	Storage (File)		
Labels	Data Domain, Compliance, PCI		

Summary

EMC Data Domain **APM00139404415** at site **London** is not enabled with remote logging.

Description

EMC Data Domain **APM00139404415** at site **London** does not have security logging enabled:

Remote logging value	ECSL logging host IP
disabled	N/A

Impact

Remote logging should be enabled and at least one ECSL logging host is specified. All logs must be time-stamped and sent to approved central syslog repository. Failing to meet this practice may lead to security audit failures and to increased risk of unauthorized access.

Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible. Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs, and they do not know that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files. By writing logs to central log servers, the risk of those logs being lost or altered is lowered, as they are more secure within the internal network.

Off-loading is a process designed to preserve the confidentiality and integrity of audit records by moving the records from the primary information system to a secondary or alternate system. It is a common process in information systems with limited audit storage capacity; the audit storage is used only in a transitory fashion until the system can communicate with the secondary or alternate system designated for storing the audit records, at which point the information is transferred.

By writing logs to central and hardened log servers, the risk of those logs being lost or altered is lowered, as they are more secure within the internal network. Without central log servers, an organization may fail to meet audit log retention and accuracy requirements.

Resolution

Enable remote logging and set at least one ECSL logging host for the array.

Risk 360

Risk ID	C00184	Name	NFSv3/4 not Enabled
Severity	ERROR	Status	OPEN
Categories	Security Compliance		
Area	Storage (File)		
Labels	Isilon, EMC, Compliance		

Summary

EMC Isilon **isdatalo55** at site **Tokyo** is not enabled with NFSv3/4.

Description

NFS settings for EMC Isilon **inycc001** at site **Tokyo** are not configured correctly:

Variable	Setting
NFSv3	Yes
NFSv4	No

Impact

Failing to meet this requirement may lead to security audit failures and to increased risk of unauthorized access. With NFSv4, the mandatory security mechanisms are oriented towards authenticating individual users, and not client machines as used in NFSv2 and NFSv3.

Resolution

The setting for the 'NFSv3 Enabled', 'NFSv4 Enabled' and 'NFS Service Enabled' should be 'Yes'.

Risk 645

Risk ID	C00727	Name	Central Log Server not Configured
Severity	ERROR	Status	REOPEN
Categories	Security Compliance		
Area	Storage		
Labels	NetApp, Audit Logging, syslog, NIST SP800-53 AU-4.1, PCI DSS 10.5.4, PCI DSS 10.5.3, ISO/IEC 27001 A.16.1.7		

Summary

NetApp filer **pdocut2file** at site **Austin** is not configured with a central log server.

Description

NetApp filer **pdocut2file** at site **Austin** does not have the required settings for log retention:

- Syslog server IP is not defined

Impact

The following Audit and Syslog logs must be retained on a schedule determined by the sensitivity and/or criticality of the data with a minimum retention policy of 6 months:

- Successful and failed administrative access
- Console commands
- IP address of client system initiating the call

All logs must be time-stamped and sent to approved central syslog repository. Failing to meet this practice may lead to security audit failures and to increased risk of unauthorized access.

Off-loading is a process designed to preserve the confidentiality and integrity of audit records by moving the records from the primary information system to a secondary or alternate system. It is a common process in information systems with limited audit storage capacity; the audit storage is used only in a transitory fashion until the system can communicate with the secondary or alternate system designated for storing the audit records, at which point the information is transferred.

By writing logs to central and hardened log servers, the risk of those logs being lost or altered is lowered, as they are more secure within the internal network. Without central log servers, an organization may fail to meet audit log retention and accuracy requirements.

Resolution

Define the syslog server IP and additional retention settings.

Risk 627

Risk ID	C00286	Name	Unsecure NetApp SNMP Community Settings
Severity	WARNING	Status	OPEN
Categories	Security Compliance		
Area	Storage (File)		
Labels	NetApp, NAS, SAN, SNMP, PCI DSS, HIPAA		

Summary

NetApp filer **nasprd101** at site **Austin** is configured with unsecure SNMP community settings.

Description

NetApp filer **nasprd101** at site **Austin** does have the required SNMP settings. SNMP should neither have "public" community nor "RW" community settings.

The following table lists the community settings:

Community setting	Community name
ro	public

Impact

The default "public" string must be changed. Writes and updates must not be allowed using SNMP. Failing to meet this requirement may lead to security audit failures and to increased risk of unauthorized access.

The SNMP Community String is like a user id or password that is sent along with each SNMP Get-Request and allows (or denies) access to a device. If the community string is correct, the device responds with the requested information.

Most network vendors ship their equipment with a default password of "public". It is recommended to change the community string to keep intruders from getting information about the network setup.

Resolution

Default string "public" must be changed. Writes/Updates must not be allowed using SNMP - remove RW community.

Risk 351

Risk ID	V00503	Name	RPA Command Injection Vulnerability
Severity	ERROR	Status	OPEN
Categories	Security Vulnerability		
Area	Data Protection Appliance		
Labels	RecoverPoint, Dell EMC, CVE		

Summary

RecoverPoint **192.23.1.42** at site **London** is exposed to a command injection vulnerability.

Description

RecoverPoint **192.23.1.42** at site **London** is installed with a vulnerable software release.

The following table lists the affected RecoverPoint system and installed vulnerable version:

RPA	Type	RecoverPoint release
192.23.1.42	RecoverPoint	5.1.0.0

Impact

Malicious user with boxmgmt privileges will be able to bypass Boxmgmt CLI and run arbitrary commands with root privileges. Refer to https://www.cvedetails.com/cve/CVE-2018-1184 for additional detail.

Resolution

Upgrade to a non-vulnerable RecoverPoint version.

Risk 81

Risk ID	C00970	Name	Unapproved Local Account
Severity	WARNING	Status	OPEN
Categories	Security Compliance	Business Entity	
Area	Storage (File)		
Labels	NetApp, IAM, Compliance, NIST SP 800-53 IA-2, CISv7 Control 16.2, HIPAA 164.312(a)(1), COBIT 5 DSS05.04, PCI DSS 8.1, ISO/IEC 27001 A.9.2, NIST SP800-53 AC-2		

Summary

NetApp cluster **tlddr1010** at site **Rochester** has unauthorized local user accounts.

Description

NetApp cluster **tlddr1010** at site **Rochester** is configured with 3 unauthorized non-default local accounts:

- ntpadmin
- jackr
- lora

The users are not listed in *ApprovedUsers.xml*.

Impact

Non-default Local accounts must not be used. Failing to meet this requirement may lead to security audit failures and to increased risk of unauthorized access.

Resolution

Remove unauthorized accounts from the storage system; replace with Active Directory user accounts as needed.

Risk 223

Risk ID	C00130	Name	Unrestricted NFS Access to root
Severity	WARNING	Status	OPEN
Categories	Security Compliance		
Area	Servers		
Labels	NetApp, Compliance, NAS, NFS, CISv7 Control 14.6, PCI DSS 7, HIPAA		

Summary

NetApp cluster **ausddr023** at site **Rochester** has unrecommended anonymous user NFS settings.

Description

NetApp cluster **ausddr023** at site **Rochester** is fails to meet the anonymous user security guidelines. A policy is configured with user ID 0 for the Anonymous user option.

The following table identifies the affected vserver and policy:

Vserver	Policy Name	User ID to Which Anonymous Users Are Mapped
ausddr023svm	open	0

Impact

An NFS mount can be advertised and mounted to allow honoring the setuid bit, but its use must be restricted to a single server or cluster of identical servers, and access controls in place so that it must not be capable of being shared to more than one system(s). Failing to meet this practice may lead to security audit failures and to increased risk of unauthorized access.

Resolution

Remove anon=0 from the NFS configuration.

Risk 283

Risk ID	C00441	Name	Ransomware Protection not Enabled
Severity	ERROR	Status	OPEN
Categories	Security Compliance		
Area	Storage (File)		
Labels	NetApp, Compliance, PCI		

Summary

NetApp cluster **tlddr1010** at site **Rochester** is not enabled with ransomware protection features.

Description

Ransomware protection features on NetApp cluster **tlddr1010** at site **Rochester** are not configured correctly -

Vserver Name	Vscan Status (pool)	FPolilcy for Ransomware file extensions
tlddr1010	Off (N/A)	N/A

Impact

Where supported by the storage system, on-access antivirus protection must be used to provide real-time identification of malware located on non-administrative CIFS/SMB file shares. Failing to meet this practice may lead to virus infections.

The NetApp **FPolicy** solution allows organizations to block traffic based on common ransomware file extensions and file metadata such as .micro .encrypted .locked .crypto .crypt .crinf .r5a, .XRNT .XTBL .R16M01D05 .pzdc .good .LOL! .OMG!, .RDM .RRK .encryptedRS .crjoker .EnCiPhErEd and .LeChiffre. Not using the fpolicy capability may increase the risk of a ransomware attack.

Resolution

Configure the antivirus to use the required configuration:

- Number of vserver = 2
- scanner-pool = SP defined for each vserver

Configure a NetApp FPolicy to block common ransomware file extensions.

Risk 1210

Risk ID	C00299	Name	Unapproved Storage Software
Severity	ERROR	Status	OPEN
Categories	Security Compliance		
Area	Storage		
Labels	VNX, SAN, NAS, Compliance		

Summary

EMC VNX **SYSVNX0011** at site **London** is installed with unapproved software.

Description

EMC VNX **SYSVNX0011** at site **London** has unapproved code:

Array name	Model	Version
SYSVNX0011	VNX5800	05.33.009.5.231

Impact

Storage systems and their underlying components must be built and updated with the latest Bank certified code with associated security updates, patches and service packs, including remediation of all GIS vulnerability assessment findings.

Resolution

Update the array software version to the approved software code.

Risk 1273

Risk ID	C00183	Name	Local User Account Control
Severity	ERROR	Status	REOPEN
Categories	Security Compliance		
Area	Storage (Block)		
Labels	VNX, Dell EMC, IAM, Compliance, NIST SP 800-53 IA-2, CISv7 Control 16.2, HIPAA 164.312(a)(1), COBIT 5 DSS05.04, PCI DSS 8.1, ISO/IEC 27001 A.9.2, NIST SP800-53 AC-2		

Summary

EMC VNX **EUR0-VNX0500** at site **London** has un-vaulted local user accounts.

Description

6 local users defined on EMC VNX **EUR0-VNX0500** at site **London** are not vaulted in CyberArk.

- tomg
- emc3
- sysadmin
- mlstorage
- stomgr

Impact

Access to a storage system must use a centralized authentication access method. In addition, Factory default local accounts must use a password vaulting solution. Failing to meet this practice may lead to security audit failures and to increased risk of unauthorized access.

Resolution

Remove un-vaulted local accounts from the switch.

[End of Report]