CONTINUITY

Risks in Detail

The following section lists the details of findings.

K0502I0MP908: Ransomware protection Policy

Security Principle	Malware scanning is enabled	**Category**	Malware Protection
System Type	NetApp cluster	**Status/Severity**	Open (ERROR)
Classification	SG-NetApp	**Areas**	Storage
		Ease of Implementation	Medium

PCI DSS	PCI DSS 5.1	ISO	ISO/IEC 27001	ISO/IEC 27001 A.12.2.1	ISO/IEC 27040
CIS Control	CIS Control 8.1	NIST	NIST SP800-53	NIST SP800-53 SI-3	NetApp (Fighting Ransomware)

Summary

Ransomware filtration is not configured.

Additional Information

The system is not configured to block ransomware attacks. File policies can be defined to block writes to an export or share that are suspected as ransomware.

Customizable parameters for this check:

- **Blocked file operations:** create
- **Known ransomware file extensions:**.14x, .1cbu1, .1txt, .52pojie, .73i87A, .a5zfn, .aaa, .abc, .adk, .aesir, .alcatraz, .AngleWare, .antihacker2017, .atlas, .axx, .Back, .BarRax, .bbawasted,.bitstak, .bmd, .bondy, .bonsoir, .booa, .boom, .boop, .braincrypt, .breaking_bad, .bript, .btc, .ccc, .cerber, .cnh, .coded, .comrade, .conficker, .copa, .coverton, .covid,.crab, .crinf, .cring, .cry, .cryeye, .CryForMe, .cryp1, .crypt, .crypte, .crypted, .crypto, .cryptolocker, .cryptowall, .crypz, .CYRAT, .czvxce, .d4nk, .dale, .damage, .darkness, .dCrypt, .deadfiles, .DeroHE, .derp, .Dexter, .dharma, .dll, .dxxd, .easyransom, .ecc, .edgel, .eduransom, .ehre, .enc, .EnCiPhErEd, .encr, .encrypt, .encrypted, .encryptedRSA, .enigma, .erif, .evillock, .exotic, .exx, .ezz, .fantom, .Fappy, .FastWind, .file0locked, .FLAMINGO, .fs0ciety, .fucked, .fun, .FUSION, .gefickt, .globe, .good, .grt, .herbst, .hnumkhotep, .hush, .info, .jigsaaw, .judge, .kernel_pid, .kernel_time, .kimcilware, .kkk, .kobos, .kook, .kostya, .krab, .kraken, .kratos, .kyra, .lcked, .LeChiffre, .legion, .lesli, .LIZARD, .lock93, .locked, .lockedv1, .locklock, .locky, .lol!, .loli, .lovewindows, .luckyday, .madebyadam, .magic, .maya, .MERRY, .MH24, .micro, .mijnal, .mnbzr, .mole, .moloch,.MRCR1, .nginxhole, .nile, .nobu, .nuclear55, .odcodc, .odin, .OMG!, .onion, .oops, .osiris, .p5tkjw, .padcrypt, .pandemic, .pay2key, .paym, .paymrss, .payms, .pays, .pdcr, .pec, .PEGS1, .perl, .PoAr2w, .potato, .powerfulldecrypt, .pstKll, .pubg, .purge, .pzdc, .R16m01d05, .r5a, .raid10, .RARE1, .razy, .rdm, .RE78P, .reco, .rekt, .remk, .rip, .rlhwasted, .RMCM1, .rmd, .rnsmwr, .rokku, .rrk, .ruby, .sage, .SecureCrypted, .serp, .serpent, .silvertor, .Spade, .spare, .spora, .spybuster, .stn, .surprise, .szf, .tcwwasted, .theworldisyours, .thor, .ttt, .unavailable, .Valley, .vbransom, .venusf, .VforVendetta, .vindows, .vvv, .vxlock, .wannacry, .wcry, .wflx, .Whereisyourfiles, .windows10, .wncry, .xati, .xienvkdoc, .XRNT, .XTBL, .xxx, .xyz, .ytbl, .ZaCaPa, .zcrypt, .zepto, .ziggy, .zimba, .zorro, .zyklon, .Zyr, .zzz, .zzzzz

Impact

Allowing ransomware to be written the shares or zones increases the risk of a successful ransomware attack. Furthermore, since shares and exports are commonly accessible to large number of endpoints, ransomware may spread faster and wider.

Resolution

Configure file policies to block traffic that is suspected as ransomware:

```
fpolicy policy event create -vserver {param1} -event-name ransomware_EVENT -protocol cifs -file-operations create rename

fpolicy policy create -vserver {param1} -policy-name ransomware_POLICY -events ransomware_EVENT

fpolicy policy scope create -vserver {param1} -policy-name ransomware_POLICY -shares-to-include * -file-extensions-to-include {param2}

fpolicy enable -vserver {param1} -policy-name ransomware_POLICY -sequence-number 2

# param1 vserver name

# param2 list of known ransomware file extensions to block
```

Affected Systems

System Name	Site	Ransomware protection
njnas02p	New Jersey	Disabled

Infinidat vulnerability: INFINIBOX-45631

Security Principle	Vulnerability identification Infinidat CVE-2021-44228	**Category**	Vulnerabilities (CVE)
System Type	Infinidat	**Status/Severity**	Open (WARNING)
Classification	SG-CVEs	**Areas**	Storage
		Ease of Implementation	Medium

CVE-2021-44228 CVE-2021-45046 CVE-2021-45105

Summary

vulnerability identified (Infinidat INFINIBOX-45631).

Additional Information

Infinidat CVE-2021-44228: Log4Shell is a security vulnerability in the Log4J software package. Further analysis is ongoing into potential exposure of InfiniBox products, and INFINIDAT will provide updates as soon as possible.

Link to source publication: https://support.infinidat.com/hc/en-us/articles/4413483145489-INFINIDAT-Support-Announcement-2021-010-Log4Shell-CVE-2021-44228

CVSS Score: 10.0

Impact

An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

Resolution

Update to version 5.0.4 (lowest) or 5.5.4.1 (highest) versions that include the log4j fixes (refer to https://support.infinidat.com/hc/en-us/articles/360002108317-InfiniBox-5-x-Release-Notes for a complete list of releases).

Affected Systems

System Name	Site	Vulnerable version
infiniprd01	-	5.0.20.0

K022E000P160: Default administrative passwords

Security Principle	Vendor-supplied default passwords are not used	**Category**	Access Control
System Type	Pure Storage	**Status/Severity**	Open (ERROR)
Classification	SG-Pure	**Areas**	Storage
		Ease of Implementation	High

FFIEC	PCI DSS	PCI DSS 2.1	Community	ISO/IEC 27040	CIS Control
CIS Control 4.2	NIST	NIST SP800-53	NIST SP800-53 IA-5		

Summary

Default passwords are used.

Additional Information

Default users of the storage system are configured with the default (factory) known passwords.

Impact

Malicious individuals (external and internal to an organization) often use vendor default settings, account names, and passwords to compromise operating system software, applications, and the systems on which they are installed. Because these default settings are often published and are well known in hacker communities, changing these settings will leave systems less vulnerable to attack. Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password.

Resolution

The following command can be used to remediate the issue:

```
pureadmin setattr --password pureuser
```

Affected Systems

System Name	Site	Users with Default Password
purefl003p2	New Jersey	pureuser/pureuser

CONTINUITY

K0719I0M0800: SAN Fabric - zone member identification

Security Principle	Secure SAN (FC) zoning used	**Category**	Access Control
System Type	Brocade	**Status/Severity**	Open (WARNING)
Classification	SG-Brocade	**Areas**	Storage
		Ease of Implementation	Low

Brocade Fibre Channel Security Best Practices	Cisco MDS 9000 Series Fabric Configuration Guide	Community	ISO/IEC 27040

Summary

Zone members are configured with unrecommended Domain, Port identification.

Additional Information

Brocade SAN switches have zone members identified using Domain, Port identification. The vendor best practice is to use pWWN for zoning.

Required zoning method: PWWN

Impact

When Domain,Port identification is used, any device physically cabled to a port could inappropriately grant storage access to an unauthorized host.
Soft zoning – Soft zoning uses filtering implemented in Fibre-Channel switches to prevent ports from being seen from outside of their assigned zones. The security vulnerability in soft zoning is that the ports may be still accessible if the user in another zone correctly guesses the Fibre-Channel address. In this case, the FC switch will place a host WWN in a zone without evaluating the port numbers in the FC switch, which were used for connection. Port World-Wide Name (PWWN) identification is considered more secure than port number identification (used in hard zoning) because any device physically connected to a port could grant storage access to an unauthorized host. **If the SAN spans across facilities with different physical security controls, and if there is a risk that physical ports could be accessed by unauthorized individuals, soft zoning may be preferable.**

Hard zoning – Hard zoning uses physical port numbers on SAN switches, thereby physically blocking access to a zone from any device outside of the zone. This type of zoning protects from WWN spoofing attacks as it does not rely on host identity. **If the organization's physical access is thoroughly protected (i.e., it is improbable that an intruder will access a physical port), this method may be preferable.**

Resolution

Reconfigure zones such that member identification is performed using PWWNs. It is recommended to back up the SAN switch configuration before applying changes.

```
zoneremove {param1}, "{param2}"
zoneadd "{param1}, "{param3}"

# param1 zone name
# param2 Aliases of D,P members to remove formatted member1;member2...; memberN
# param3 Aliases of PWWN members to add

Note: use cfgsave and cfgenable commands to save your changes and make them the effective configuration.
```

Affected Systems

System Name	Zone	Ports
sanfcdir0a	zo_esx_flash_a_3c	1,82
sanfcdir0a	zo_lin_flash_b_4f	2,10

CONTINUITY

K080CI00P183: Protected recovery copies

Security Principle	Immutable data copies	**Category**	Malware Protection
System Type	Data Domain	**Status/Severity**	Open (ERROR)
Classification	SG-Data Domain	**Areas**	Storage
		Ease of Implementation	Low

FFIEC ISO/IEC 27040 SEC Rule 17a-4 Dell EMC Ransomware Protection NIST SP800-209 IS-SS-R10

Summary

File retention lock option is disabled.

Additional Information

Data Domain retention lock functionality ensures backup cannot be deleted during the retention period. Once enabled, the data is retention locked to further protect it from accidental or intentional deletion or ransomware for example.

Impact

An attacker obtaining administrative access could delete backup copies and make recovery of data impossible.

Resolution

Review backup software documentation for integration options with EMC Data Domain retention lock functionality. Use the following commands to configure retention lock:

```
mtree retention-lock set min-retention-period {param1} mtree {param2}
mtree retention-lock set max-retention-period {param3} mtree {param4}
system retention-lock compliance configure #reboots the system
# param1 min period (example: 1min, 1hr, 1day, 1mo, 1year)
# param2 mtree name
# param3 max period (example: 1min, 1hr, 1day, 1mo, 1year)
# param4 mtree name
```

Affected Systems

System Name	Site	Retention Lock status
eddbk003	Tokyo	disabled

K140D00MP345: File share client access list

Security Principle	Access rights granted to authorized users/hosts only	**Category**	Authorization
System Type	Isilon	**Status/Severity**	Open (WARNING)
Classification	SG-Isilon	**Areas**	Storage

PCI DSS	PCI DSS 7.1	Community	ISO/IEC 27040	CIS Control	CIS Control 4.1
NIST	NIST SP800-171	NIST SP800-53	NIST SP800-53 AC-2		

Summary

Access to file shares is not restricted by client IP.

Additional Information

Shares on EMC Isilon storage system are not restricted to specific client IP addresses. The list of clients with access through these exports is unlimited (0.0.0.0).

Impact

The more people who have access to data, the more risk there is that a user's account will be used maliciously. Limiting access to those with a legitimate business reason for the access helps an organization prevent mishandling of data through inexperience or malice.

Resolution

Add the IP addresses of the specific clients requiring access to the NFS share. Then, use the following command to remove the unrestricted access configuration:

```
isi nfs exports modify {param1} --remove-clients 0.0.0.0
isi nfs exports modify {param1} --remove-root-clients 0.0.0.0
isi nfs exports modify {param1} --remove-read-write-clients 0.0.0.
# param1 nfs export id number
```

Affected Systems

System Name	Site	Client access configuration
Isiprd03bl	Birmingham	/ifs/data/gr/dwht1_data/dbdkj4: RW Clients: 0.0.0.0 /ifs/data/gr/certsto/sq0458d: RW Clients: 0.0.0.0

K2102I000965: Snapshot autodelete configuration

Security Principle	Immutable data copies	**Category**	Malware Protection
System Type	NetApp cluster	**Status/Severity**	Open (ERROR)
Classification	SG-NetApp	**Areas**	Storage
		Ease of Implementation	Medium

FFIEC ISO/IEC 27040 SEC Rule 17a-4 NetApp (Fighting Ransomware)

Summary

Snapshot autodelete is enabled.

Additional Information

Automatic snapshot deletion is enabled for data volumes of the storage system. The vendor security recommendation is to disable automatic snapshot deletion.

Impact

Ransomware creates a high rate of change data because it encrypts the file system.
The storage system holds all of the encrypted data and the original unencrypted data in Snapshot copies. Although snapshot autodelete is a great feature to keep volumes from filling all the way up, during a ransomware attack you would rather have a volume that is full and still includes recoverable Snapshot copies than a volume with only ransomware-encrypted data and no recoverable copies.
You can configure volume auto-size to grow volumes that are nearly full to prevent them from filling up. When the volume is nearly full, you can set up an alert using thresholds.

Resolution

NOTE: NetApp recommends configuring volume autosize to grow volumes that are nearly full to prevent them from filling up. When the volume is nearly full, you can set up an alert using thresholds.

The following command can be used to disable Snapshot autodelete:

```
volume snapshot autodelete modify -vserver {param1} -volume {param2} enabled false
# param1 vserver name
# param2 volume name
```

Affected Systems

System Name	Site	is-autodelete-enabled=true
nynas05p	New York	FIN0001_data_t1p

CONTINUITY

K020CI0MP298: IPFilter configuration

Security Principle	Management access is restricted	**Category**	Access Control
System Type	Data Domain	**Status/Severity**	Open (ERROR)
Classification	SG-Data Domain	**Areas**	Storage
		Ease of Implementation	High

CIS Control | CIS Control 9.4 | NIST SP800-209

Summary

IPFilter is not configured to restrict access to the system.

Additional Information

The system is not configured with access list defining allowed client IP addresses. Administrative access is not restricted to a list of trusted storage management clients.

Impact

Attackers search for remotely accessible network services that are vulnerable to exploitation. Restricting access to storage management only to authorized client IPs can significantly reduce the attack surface.

Resolution

The following command can be used to define IP filtering:

```
net filter add [seq-id n] operation {allow | block} [clients {host-list | ipaddr-list}] [except-clients
{host-list | ipaddrlist}] [interfaces {ifname-list | ipaddr-list}] [exceptinterfaces {ifname-list |
ipaddr-list}] [ipversion {ipv4 | ipv6}]


# example 1 - only allows specific hosts to use SSH to the target Data Domain system on management
interface ethV0:

## net filter add seq-id 1 operation block protocol tcp ports 22 interfaces ethV0 ipversion ipv4
except-clients {crHostIP}


# example 2 - disable SSH on the replication interface:

## net filter add seq-id 2 operation block protocol tcp ports 22 interfaces ethV1 ipversion ipv4
```

Affected Systems

System Name	Site	Violation		
eddbk003	Tokyo	IPv4 admin-interface	22,443	all clients
		IPv6 admin-interface	22,443	all clients

K0110I0MP0734: Command Device (CLI) Authentication

Security Principle	Strong storage management host identification	**Category**	Access Control
System Type	Hitachi	**Status/Severity**	Open (ERROR)
Classification	SG-Hitachi	**Areas**	Storage
		Ease of Implementation	Medium

Hitachi Vantara

Summary

Command device authentication is not used.

Additional Information

The storage system is configured with command devices for which user authentication is not required. When user authentication is enabled for the command devices, only commands issued by authorized users can be executed.

Customizable parameters for this check:

- **Command device user authentication:** enable
- **Scope (Regex):** N/A

Impact

Unauthorized users will be able to issue commands to the storage systems and adversely affect data integrity, accessibility, availability or security.

Resolution

The following command can be used to change authentication mode of command device:

```
HiCommandCLI {param1} ModifyLogicalUnit model={param2} serialnum={param3} devnum={param4}
commanddevice=true commanddeviceauth=true

# param1 URL

# param2 model

# param3 serial number

# param4 device number
```

NOTE: In certain versions, when you change the settings of the command device by using the CLI ModifyLogicalUnit command of Device Manager, if you specify the commandDeviceSecurity parameter, the commandDeviceAuth settings may become disabled. Additionally, if you edit the command device in Replication Manager, the user authentication settings may become disabled. It's important to continuously validate secure configuration is in place.

Affected Systems

System Name	Site	Command device
50039	New Jersey	LU.R800. 50039.39088

IBM V7000/SVC vulnerability: 872456

Security Principle	Vulnerability identification IBM V7000/SVC 872456	**Category**	Vulnerabilities (CVE)
System Type	IBM V7000/SVC	**Status/Severity**	Open (WARNING)
Classification	SG-CVEs	**Areas**	Storage
		Ease of Implementation	Medium

CVE-2018-1517 CVE-2018-2783 CVE-2018-12539

Summary

vulnerability identified (IBM V7000/SVC 872456).

Additional Information

Vulnerabilities in the IBM Runtime Environment Java Technology Edition affect IBM SAN Volume Controller, IBM Storwize V7000, V5000, V3700 and V3500, IBM Spectrum Virtualize Software, IBM Spectrum Virtualize for Public Cloud and IBM FlashSystem V9000 and 9100 family products. The applicable CVEs are CVE-2018-1517, CVE-2018-2783 and CVE-2018-12539.

Link to source publication: https://www.ibm.com/support/pages/security-bulletin-multiple-vulnerabilities-ibm-java-sdk-affect-ibm-san-volume-controller-ibm-storwize-ibm-spectrum-virtualize-and-ibm-flashsystem-products

CVSS Score: 8.4

Impact

The vulnerabilities may allow an attacker to inflict a denial-of-service attack with specially crafted String data, also attacker could exploit vulnerability to execute untrusted native code and gain elevated privileges on the system, allowing an unauthenticated attacker to cause high confidentiality impact and high integrity impact.

Resolution

Upgrade the system to release 8.2.1 or above.

Affected Systems

System Name	Site	Vulnerable version
svcprd596tl	New Jersey	8.1.3.6

K030CIVM0365: CIFS SMBv1 status

Security Principle	Unsecure SMB versions are disabled	**Category**	Services and Protocols
System Type	Unity	**Status/Severity**	Open (ERROR)
Classification	SG-Unity	**Areas**	Storage
		Ease of Implementation	High

ISO/IEC 27040 Microsoft NIST SP800-209 NC-SS-R19 CISA Ransomware Guide

Summary

SMBv1 is enabled.

Additional Information

A vulnerable SMB version is enabled on the storage system. Threat actors use SMB to propagate malware across organizations.

Impact

SMBv1 is highly vulnerable and should not be used. For example, Wannacry and Petya are forms of malware that took advantage of SMBv1 weaknesses.

Resolution

The following command can be used to disable SMB1:

```
svc_param ALL -f cifs -m smb1.disabled -v 1
```

NOTE: Analyze and mitigate any existing dependencies that may break before disabling SMBv1.

Affected Systems

System Name	Site	SMB1 status
emcnasuty11	Birmingham	Enabled

[End of Report]