CISCO SD-WAN THREAT HUNT GUIDE

February 2026

Version 2.4

National Cyber Security Centre NEW ZEALAND | Te Tira Tiaki Government Communications Security Bureau

Communications Security Establishment Canada | Canadian Centre for Cyber Security | Centre de la sécurité des télécommunications Canada | Centre canadien pour la cybersécurité

AUSTRALIAN SIGNALS DIRECTORATE 1947-2022 75 REVEAL AND PROTECT

National Cyber Security Centre a part of GCHQ

Australian Government Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE ACSC Australian Cyber Security Centre

Contents

Cisco SD-WAN Threat Hunt Guide 3

Tradecraft Overview 4

- **Initial Access** 4
- **Privilege Escalation** 4
- **Lateral Movement** 5
- **Defense Evasion** 6

Detection Planning 7

- **Devices of Focus** 7
- **Artefacts to Collect** 7
- **Detection Overview** 7

Detections 8

- **PRIVESC-T1601.002-AppDowngrade-001** 8
- **PRIVESC-T1601.002-AppReversion-002** 10
- **INITIALACCESS-T1190-PeerTimeouts-003** 11
- **INITIALACCESS-T1190-PeerTypeAnom-004** 12
- **INITIALACCESS-T1190-RoguePeerOutlier-005** 13
- **INITIALACCESS-T1190-RemoteColorNull-006** 15
- **INITIALACCESS-T1190-DumpPkt-007** 16
- **INITIALACCESS-T1190-SiteIDAnom-008** 16
- **INITIALACCESS-T1190-GetCARSAKey-009** 17

INITIALACCESS-T1190-PeerCertFail-010 19
PRIVESC-T1068-CVE202220775-011 20
PERSISTENCE-T1098.004-RootSSHKeyAccepted-012 22
PERSISTENCE-T1098.004-vmanage-adminSSHAuthorizedKey-012b 23
PERSISTENCE-T1078-RootOrRogueLogins-013 23
PERSISTENCE-T1136.001-UserAddAAA-014 24
PERSISTENCE-T1098.004-PermitRootLogin-015 25
LATERALMOVE-T1021.004-KnownHosts-016 26
PERSISTENCE-T1136.001-RollbackUserOps-017 27
PRIVESC-T1601.002-RollbackCounterReset-018 28
DEFENSEEVASION-T1070.003-BashVsCliHistory-019 30
DEFENSEEVASION-T1070.002-ClearLoginLogs-020 31
DEFENSEEVASION-T1070.007-SearchRogueIP-021 32
DEFENSEEVASION-T1070.003-ClearShellHistory-022 33
PERSISTENCE-T1098.004-RootDiskArtefacts-023 33
CREDENTIALACCESS-T1110-PamFaillock-024 36
Mitigations 37
Use the "Golden Star" SD-WAN Version 37
Patch the SD-WAN 37
Network Filtering 37
Data Plane Security 37
Centralised Logging 37
Disclaimer 38
Glossary 38
Detection table standards 39
Traffic Light Protocol 40

Cisco SD-WAN Threat Hunt Guide

The authors are aware that since 2023, at least one malicious cyber actor compromised Cisco SD-WANs via a previously unknown vulnerability, identified in late 2025 to be a zero-day exploit. This vulnerability is now patched in the latest updates from the vendor.

The vulnerability allowed a malicious cyber actor to create a rogue peer joined to the network management plane, or control plane, of an organisations SD-WAN. The rogue device

appears as a new but temporary, actor-controlled SD-WAN component that can conduct trusted actions within the management and control plane.

The purpose of this guide is to assist organisations in investigating their Cisco Software-Defined Wide Area Network (SD-WAN) [1] for indicators of cyber compromise. The guide is written for cybersecurity professionals and network administrators that utilise Cisco SD-WAN technology.

All activity observed was limited to the SD-WAN components and lateral movement outside the SD-WAN was not seen by investigators.

Tradecraft Overview

The following is a summary of key tactics used by the malicious cyber actor. MITRE ATT&CK framework v18 references are provided where possible.

Initial Access

T1190 Exploit Public Facing Application[2]

The vulnerability allows the actor to add a rogue peer to the Cisco SD-WAN management and control plane. The rogue peer is an actor controlled, unauthorised, now trusted peer on the SD-WAN network management system (NMS).

This rogue peer receives an IP address in the NMS management plane VPN512 and allows the attacker to interact with management and control devices within that restricted management plane through the now trusted, but rogue peer.

Privilege Escalation

T1601.002 Modify System Image: Downgrade[3]

Using the built-in update mechanism, the actor downgraded a vSmart controller to a version with publicly known local privilege escalation vulnerabilities. Post exploitation, achieving privilege escalation to and persistence as the user 'root', the actor restored the vSmart (controller) to the version it was running before it was downgraded to the vulnerable version. The downgrade activity created significant logging and is recorded in the detections section.

---

[1] Be aware that in 2023 Cisco rebranded components within the SD-WAN. This document refers to 'vManage', now known as 'manager'; 'vSmart', now known as 'controller'; and 'vBond', now known as a 'validator'. This guide will collectively refer to these products as the SD-WAN Network Management System (NMS).

[2] Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®

[3] Modify System Image: Downgrade System Image, Sub-technique T1601.002 - Enterprise | MITRE ATT&CK®

T1068 Exploitation for Privilege Escalation[4]

Immediately after the system downgrade, the actor exploited the local privilege escalation vulnerability CVE-2022-20775[5]. The actor used what was likely a publicly available proof of concept exploit for this CVE to run commands as the root user.

Persistence

The actor persisted primarily through local accounts, and relying on re-exploiting the zero-day rogue peer for interactive sessions. No command-and-control malware was discovered by investigators.

T1190 Exploit Public Facing Application

Responders observed rogue peering events occurring whenever the actor conducts an interactive session within the SD-WAN. The actor achieved this through the rogue peer zero-day exploit.

T1136.001 Create Account: Local Account[6]

The actor created local user accounts that mimicked other local user accounts.

T1098.004 Account Manipulation: Secure Shell Protocol Authorized Keys[7]

After privilege escalation, the actor added a Secure Shell Protocol (SSH) authorized key for root access.

It is likely that the actor added an authorized key for '`vManage-admin`' during the rogue peering exploit script.

T1037 Boot or Logon Initialization Scripts[8]

Using root access, the actor modified SD-WAN related start-up scripts to customise the environment.

Lateral Movement

Lateral movement has not been observed outside the Cisco SD-WAN environment. The methods described below are from the rogue peer to other devices in the SD-WAN management plane.

---

[4] Exploitation for Privilege Escalation, Technique T1068 - Enterprise | MITRE ATT&CK®

[5] Cisco SD-WAN Software Privilege Escalation Vulnerabilities - Cisco

[6] Create Account: Local Account, Sub-technique T1136.001 - Enterprise | MITRE ATT&CK®

[7] Account Manipulation: SSH Authorized Keys, Sub-technique T1098.004 - Enterprise | MITRE ATT&CK®

[8] Boot or Logon Initialization Scripts, Technique T1037 - Enterprise | MITRE ATT&CK®

T1021.004 Remote Services: SSH[9]

The actor used Network Configuration Protocol on port 830 (NETCONF) and SSH to connect to/between Cisco SD-WAN appliances within the management plane.

The actor likely used the web interface of the SD-WAN manager to perform operations on the SD-WAN.

Defense Evasion

The actor consistently applied defence evasion techniques, primarily related to removing forensic artifacts on the host.

T1070.002 Indicator Removal: Clear Linux or Mac System Logs[10]

The actor cleared items under `/var/log`. This log clearing is very effective if the actor has root access.

T1070.003 Clear Command History[11]

The actor typically cleared shell history for any masqueraded or actor-controlled user. This includes both the restricted SD-WAN shell and the operating system shell.

T1070.007 Indicator Removal: Clear Network Connection History and Configurations[12]

The author authenticated to, searched for, and removed specific entries from the vManage Elasticsearch database, to remove evidence of their attack.

Specific clearing included their rogue peer internal IP address.

T1562.006 Indicator Blocking

The actor disabled a network interface on NMS components that was used to send syslog messages. This action prevents logging being forwarded to an external server.

---

[9] Remote Services: SSH, Sub-technique T1021.004 - Enterprise | MITRE ATT&CK®

[10] Indicator Removal: Clear Linux or Mac System Logs, Sub-technique T1070.002 - Enterprise | MITRE ATT&CK®

[11] Indicator Removal: Clear Command History, Sub-technique T1070.003 - Enterprise | MITRE ATT&CK®

[12] Indicator Removal: Clear Network Connection History and Configurations, Sub-technique T1070.007 - Enterprise | MITRE ATT&CK®

Detection Planning

Devices of Focus

The actor focused on the vSmart and vManage appliances within the NMS. In the early stages of intrusion, the actor focused on vSmart.

Artefacts to Collect

System logging, combined with log forwarding, is enough to detect compromise. The logs must be forwarded off the appliance to a centralised logging solution to evade log event clearing by the actor.

For local installations, disk and memory images provide unique insights. If virtualised, collect by creating a snapshot of the virtual appliances at the hypervisor.

For cloud and local installations, an Admin-Tech dump can provide a useful all in one collection to triage[13].

Detection Overview

To identify compromise of your Cisco SD-WAN, focus detections on the following activities:

- Rogue peering
- Version downgrade and unexpected reboot events
- SSH abuse
- Root SSH and Root login anomalies
    - The root user login is locked down in Cisco SD-WANs and should never be used interactively.
    - Any artefacts generated from root login and timestamps could provide a valuable pivot point.
- Command line history analysis

[13] https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/216954-how-to-collect-an-admin-tech-in-an-sd-wa.html#toc-hId--321285228),

Detections

The following detections relate to tradecraft described in the overview in enough detail to enable the generation of detections relevant to your system.

The structured tables will enable some automated translation to structured SIEM rules if desired.

PRIVESC-T1601.002-AppDowngrade-001

title	Application Downgrade
id	PRIVESC-T1601.002-AppDowngrade-001
status	experimental
description	Detects a software downgrade on vSmart that often precedes privilege escalation to root. Downgrades typically trigger a reboot and generate distinctive sw_script/cdb_set version-change artefacts.
references	Cisco SD-WAN Threat Hunt Guide – Activity 1 & 2 (source document)
tags	attack.t1601.002
logsource	product: Cisco SD-WAN service: vSmart (controller) category: application, system paths: /var/log/tmplog/vdebug, /var/volatile/log/vdebug, /var/volatile/log/sw_script_synccdb.log
detection	Sequence (≈15–30m window): 1) 'cdb Set software <older_version>' events indicating activation of an older image; 2) associated 'sw' master-install initialisation; 3) reboot artefacts (reboot notice, daemon shutdowns, service re-initialisation).
conditions	• message contains 'cdb_set: cdb Set software' AND ('active true' OR 'default false' OR 'previous false') • process contains 'sw' AND message contains 'master install' • Reboot markers such as 'system-reboot-issued' and service restarts
falsepositives	• Administrator-driven rollback • Failed upgrade causing fallback to previous image
level	high

analytic_validation	Confirm image version change vs authorised plan; verify reboot artefacts; pivot to 'Application Reversion After Downgrade'; check for subsequent privilege-escalation (CVE-2022-20775).
samples	`Content Modification Time,LOG,Log File,[sw] cdb_set: cdb Set software 20.6.1/active true successful` `Content Modification Time,LOG,Log File,[sw] cdb_set: cdb Set software 20.6.1/default false successful` `Content Modification Time,LOG,Log File,[sw] cdb_set: cdb Set software 20.6.1/previous false successful` `Content Modification Time,LOG,Log File,[sw] cdb_set: cdb Set software 20.6.1/timestamp <TIMESTAMP> successful`
related	PRIVESC-T1601.002-AppReversion-002, PRIVESC-T1068-CVE202220775-012

PRIVESC-T1601.002-AppReversion-002

title	Application Reversion After Downgrade
id	PRIVESC-T1601.002-AppReversion-002
status	experimental
description	Detects timed reversion prompts following a malicious downgrade; actor fails to confirm upgrade, triggering automatic reversion.
references	
tags	attack.t1601.002
logsource	product: Cisco SD-WAN service: vSmart (controller) category: application paths: /var/log/tmplog/vdebug
detection	Within 15 minutes of a downgrade: look for upgrade confirmation timer messages and 'Software upgrade not confirmed' resulting in reversion.
conditions	• message contains 'Starting upgrade confirmation timer' • message contains 'Waiting for upgrade confirmation from user' • message contains 'Software upgrade not confirmed'
falsepositives	• None observed outside malicious downgrade windows; validate against approved change window
level	high
analytic_validation	Correlate with Detection 001 (downgrade). Verifying timer/reversion messages occur only in malicious windows per source observations.
samples	`[vScript] Starting upgrade confirmation timer (15 mins)` `[vScript] %%Viptela-vsmart1-SYSMGR-5-NTCE-200059: Waiting for upgrade confirmation from user. Device will revert to previous software version 20.9.5.1 in '100' seconds unless confirmed.` `[vScript] %%Viptela-vsmart1-SYSMGR-5-NTCE-200049: Software upgrade not confirmed. Reverting to previous software version 20.9.5.1`
related	PRIVESC-T1601.002-AppDowngrade-001, PRIVESC-T1068-CVE202220775-012

INITIALACCESS-T1190-PeerTimeouts-003

title	Control Peer Timeouts Spike
id	INITIALACCESS-T1190-PeerTimeouts-003
status	test
description	Hunt for increased or low frequency 'ssl shutdown' and 'Timing out peer' messages by PID aggregation; can align with rogue peering but not definitive.
references	
tags	attack.t1190
logsource	product: Cisco SD-WAN service: vSmart (controller) category: application, network paths: /var/log/tmplog/vdebug
detection	Aggregate by PID over a hunt window; flag low-frequency occurrences of 'Received ssl shutdown from peer' and 'Timing out peer'.
conditions	• message contains 'Received ssl shutdown from peer' • message contains 'Timing out peer'
falsepositives	• Background network churn; transient control-plane instability
level	low
analytic_validation	Use only as supporting signal. Correlate temporally with higher-fidelity rogue peering analytics (004–009).
samples	`[VDAEMON_3 pid: 2972] vbond_peer_timer_exp_cb[205]: %VDAEMON_DBG_ERROR-1: Timing out peer <IP|PORT> on eth0` `[VDAEMON_3 pid: 2972] vdaemon_tls_post_connect_eventcb[296]: %VDAEMON_DBG_MISC-1: Received ssl shutdown from peer (<IP|PORT>). Deleting peer`
related	INITIALACCESS-T1190-PeerTypeAnom-004, INITIALACCESS-T1190-RoguePeerOutlier-005

INITIALACCESS-T1190-PeerTypeAnom-004

title	Anomalous Peer Type
id	INITIALACCESS-T1190-PeerTypeAnom-004
status	stable
description	Flags rogue peering when 'peer-type' exhibits anomalous values seen in incidents (e.g., 'vhub') in control-connection state changes on vSmart; use frequency/outlier analysis when specific invalid values are not known.
references	
tags	attack.t1190
logsource	product: Cisco SD-WAN service: vSmart (controller) category: application, network paths: /var/log/tmplog/vdebug
detection	Select 'control-connection-state-change' events where (peer-type:'vhub' as observed) OR peer-type appears as a low-frequency outlier, especially with new-state:up and uptime '0:00:00:00'.
conditions	• message contains 'control-connection-state-change' • (peer-type == 'vhub') OR frequency(peer-type) is low • message contains 'new-state:up'
falsepositives	• Introduction of new roles/peers in testing or upgrades (rare) • Short-lived lab connections
level	high
analytic_validation	Confirm peer is unauthorised in inventory; correlate with remote-color anomaly, dump_pkt, or malformed hello within the same minute.
samples	`[VDAEMON_0 pid: 2852] %Viptela-vsmart1-vdaemon_0-6-INFO-1400002: Notification: control-connection-state-change severity-level:major host-name:"vsmart1" system-ip:<REDACTED IP>personality:vsmart peer-type:vhub peer-system-ip:<REDACTED IP> peer-vmanage-system-ip:0.0.0.0 public-ip:<ACTOR IP> public-port:41942 src-color:default remote-color:default uptime:"0:00:00:00" new-state:up`

related	INITIALACCESS-T1190-RoguePeerOutlier-005, INITIALACCESS-T1190-RemoteColorNull-006, INITIALACCESS-T1190-DumpPkt-007

INITIALACCESS-T1190-RoguePeerOutlier-005

title	**Rogue Peering Outlier Cluster**
id	INITIALACCESS-T1190-RoguePeerOutlier-005
status	experimental
description	Uses joint frequency of 'peer-type' and 'peer-system-ip' to identify small clusters of rogue peers; parameterise to focus on 'peer-type:vmanage' where helpful.
references	
tags	attack.t1190
logsource	product: Cisco SD-WAN service: vSmart (controller) and vManage (manager) category: application, network paths: /var/log/tmplog/vdebug, /var/log/vsyslog, /var/log/jsyslog, /var/log/messages
detection	Group by (peer-type, peer-system-ip); count and sort ascending; investigate low-count pairs, especially with 'new-state:up' and short uptimes.
conditions	• aggregation: group fields peer-type, peer-system-ip • threshold: count <= small N (environment-specific) • optional filter: peer-type:'vmanage' and unexpected ip
falsepositives	• Ephemeral test peers; short-lived maintenance connections
level	high
analytic_validation	Validate unexpected peer-system-ip against asset inventory; compare public-ip frequency; pivot to related anomalies (006–009).
samples	peer-type:vmanage peer-system-ip::<rogueIP> count=3 peer-type:vmanage peer-system-ip:<vmanageIP> count=204 From logs like: `[VDAEMON_0 pid: 2969] %Viptela-vsmart1-vdaemon_0-6-INFO-1400002: Notification: control-connection-state-change severity-level:major host-`

	name:""vsmart1"" system-ip:<REDACTED IP> personality:vsmart peer-type:vmanage peer-system-ip:<rogueIP> peer-vmanage-system-ip:0.0.0.0 public-ip:<ACTOR IP> public-port:53974 src-color:default remote-color:default uptime:""0:00:00:00"" new-state:up
related	INITIALACCESS-T1190-PeerTypeAnom-004, INITIALACCESS-T1190-RemoteColorNull-006

INITIALACCESS-T1190-RemoteColorNull-006

title	Remote-Color Null on Control Connection
id	INITIALACCESS-T1190-RemoteColorNull-006
status	experimental
description	Detects initial rogue peering where 'remote-color' is null or malformed (e.g., '(null)' or '{28 0}') in control-connection events.
references	
tags	attack.t1190
logsource	product: Cisco SD-WAN service: vSmart (controller) category: application paths: /var/volatile/log/vconfd.10, /var/log/tmplog/vdebug.5
detection	Select control-connection events with remote-color equal to '(null)' or '{28 0}', especially at first peering instances.
conditions	• message contains 'control-connection-state-change' • remote-color in ['(null)', '{28 0}']
falsepositives	• Unknown; treat as high signal when temporally aligned with other rogue peering indicators
level	high
analytic_validation	Validate this appears only in initial peering; later events often show 'remote-color: default'.
samples	`[VDAEMON_0 pid: 2852] %Viptela-vsmart2-vdaemon_0-6-INFO-1400002: Notification: control-connection-state-change severity-level:major host-name:""vsmart2"" system-ip:<IP> personality:vsmart peer-type:vhub peer-system-ip:<IP> peer-vmanage-system-ip:0.0.0.0 public-ip:<IP> public-port:12346 src-color:default remote-color:(null) uptime:""0:00:00:00"" new-state:up`  `[confd pid: 2785] devel-c Failed to send notification for stream viptela: /control-connection-state-change/remote-color: {28 0}: 0 is not a valid value.`
related	INITIALACCESS-T1190-PeerTypeAnom-004, INITIALACCESS-T1190-DumpPkt-007

INITIALACCESS-T1190-DumpPkt-007

title	VDAEMON Debug Packet Post-Peering
id	INITIALACCESS-T1190-DumpPkt-007
status	experimental
description	Detects VDAEMON dbg_pkt lines (e.g., 'VDAEMON_DBG_PKT', 'vbond_dump_pkt') shortly after rogue peering; often scrubbed at rest, so rely on remote logging. Only ever observed alongside active exploitation.
references	
tags	attack.t1190
logsource	product: Cisco SD-WAN service: vSmart (controller) category: application, network paths: /var/log/tmplog/vdebug
detection	Filter for 'vbond_dump_pkt' or 'VDAEMON_DBG_PKT' lines in the minute following control-connection 'new-state:up' events with short uptime.
conditions	• message contains 'vbond_dump_pkt' OR 'VDAEMON_DBG_PKT' • time diff <= 1 minute from related peering event
falsepositives	• None known
level	high
analytic_validation	Confirm preceding rogue peering indicators and short-lived sessions.
samples	`[VDAEMON_0  pid: 2852] vbond_dump_pkt[160]: %VDAEMON_DBG_PKT-1:  RX <ACTOR IP>/41942 --> <REDACTED IP>/23456`
related	INITIALACCESS-T1190-PeerTypeAnom-004, INITIALACCESS-T1190-RemoteColorNull-006

INITIALACCESS-T1190-SiteIDAnom-008

title	Malformed Hello Site-ID
id	INITIALACCESS-T1190-SiteIDAnom-008

status	experimental
description	Flags anomalous 'Site-ID' values (e.g., '100') seen alongside VDAEMON debug hello messages during rogue peering.
references	
tags	attack.t1190
logsource	product: Cisco SD-WAN service: vSmart (controller) category: application, network paths: /var/log/tmplog/vdebug
detection	Search VDAEMON debug hello messages for atypical or environment-invalid Site-ID values.
conditions	• message contains 'vbond_dump_pkt' AND 'Msg: Hello' • message contains 'Site-ID: 100' (example; parameterise)
falsepositives	• Unlikely if Site-ID ranges are stable; validate ranges per environment
level	high
analytic_validation	Confirm Site-ID length/range against overlay inventory; correlate with other rogue peering artefacts.
samples	`[VDAEMON_0 pid: 2852] vbond_dump_pkt[171]: %VDAEMON_DBG_PKT-1: Msg: Hello Ver: 0 Device: vHub Site-ID: 100 Domain-ID: 1 MsgLen: 91`
related	INITIALACCESS-T1190-DumpPkt-007, INITIALACCESS-T1190-PeerTypeAnom-004

INITIALACCESS-T1190-GetCARSAKey-009

title	**Unexpected CA RSA Public Key Fetch (vSmart)**
id	INITIALACCESS-T1190-GetCARSAKey-010
status	test
description	Detects 'Get CA RSA Public key' on vSmart immediately after peering; common on vBond, so filter is required to reduce false positives.

references	
tags	attack.t1190
logsource	product: Cisco SD-WAN service: vSmart (controller) category: application paths: /var/log/tmplog/vdebug
detection	Select 'Get CA RSA Public key' events sourced from vSmart within a minute after a control-connection 'new-state:up' event.
conditions	• message contains 'Get CA RSA Public key' • time diff <= 1 minute from related peering event
falsepositives	• Legitimate CA key fetches (common on vBond)
level	medium
analytic_validation	Constrain to vSmart context; correlate to other rogue peering indicators.
samples	`[VDAEMON_0 pid: 2900] vbond_handshake_event_cb[1059]: %VDAEMON_DBG_MISC-1: Get CA RSA Public key`
related	INITIALACCESS-T1190-PeerTypeAnom-004, INITIALACCESS-T1190-RoguePeerOutlier-005

INITIALACCESS-T1190-PeerCertFail-010

title	Peer Certificate Validation Failure
id	INITIALACCESS-T1190-PeerCertFail-011
status	experimental
description	Detects control-connection authentication failures due to missing serial numbers during rogue peering (e.g., ERR_SER_NUM_NT_PRESENT).
references	
tags	attack.t1190
logsource	product: Cisco SD-WAN service: vSmart (controller) category: application, auth paths: /var/log/tmplog/vdebug
detection	Select 'control-connection-auth-fail' events with reasons including 'ERR_SER_NUM_NT_PRESENT' or messages indicating 'Certificate validation Failed: Unable to find the serial no'.
conditions	• message contains 'control-connection-auth-fail' • reason contains 'ERR_SER_NUM_NT_PRESENT' OR message contains 'Unable to find the serial no'
falsepositives	• Misconfigured or newly onboarded devices lacking serial registration
level	high
analytic_validation	Validate timing with suspected rogue peering; confirm device was not in onboarding.
samples	`[VDAEMON_0 pid: 2969] %Viptela-vsmart1-vdaemon_0-6-INFO-1400002: Notification: control-connection-auth-fail severity-level:major host-name:"vsmart1" system-ip:<REDACTED IP> personality:vsmart peer-type:vmanage peer-system-ip::: local-system-ip:<REDACTED IP> local-color:default reason:"ERR_SER_NUM_NT_PRESENT`  `[VDAEMON_0 pid: 2969] vdaemon_dtls_verify_peer_cert[1206]: %VDAEMON_DBG_MISC-1: Certificate validation Failed: Unable to find the serial no in the vSmart DB <REDACTED SERIAL> <REDACTED SDWAN NAME>`

related	INITIALACCESS-T1190-PeerTypeAnom-004, INITIALACCESS-T1190-RoguePeerOutlier-005

PRIVESC-T1068-CVE202220775-011

title	**Local Privilege Escalation via CVE-2022-20775**
id	PRIVESC-T1068-CVE202220775-012
status	stable
description	Detects exploitation of CVE-2022-20775 observable as a 'system-login-change' with a crafted user-name path traversal string (e.g., '/../../'), enabling root commands.
references	https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-sd-wan-priv-E6e8tEdF.html
tags	attack.t1068
logsource	product: Cisco SD-WAN service: vSmart (controller) category: auth, application paths: /var/log/tmplog/vdebug
detection	Select 'system-login-change' events where user-name matches regex ^["']?/(\.\./){2,} or contains '/tmp/pwn'. Correlate with recent downgrade.
conditions	• message contains 'system-login-change' • user-name matches '/(\.\./){2,}.*' OR message contains '/tmp/pwn'
falsepositives	• None expected under normal operations
level	critical
analytic_validation	Verify device version change around event; inspect for root shell and SSH key artefacts; exclude legitimate TAC workflows.
samples	`[SYSMGR pid: 900] %Viptela-vsmart1-sysmgrd-6-INFO-1400002: Notification: system-login-change severity-level:minor host-name:\"vsmart1\" system-ip:<IP> user-name:\"/` `&../` `&../`

	&..%2f &..%2f &tmp%2fpwn\" Note the string has been broken up by newlines and the character '&' to avoid AV hits on this document. There were some issues with some AV picking up a directory traversal attempt.
related	PRIVESC-T1601.002-AppDowngrade-001, PERSISTENCE-T1098.004-RootSSHKeyAccepted-013

PERSISTENCE-T1098.004-RootSSHKeyAccepted-012

title	Root SSH Public Key Accepted
id	PERSISTENCE-T1098.004-RootSSHKeyAccepted-013
status	stable
description	Detects SSH authentication using a public key for the root account. Often observed via remote syslog; local logs may be scrubbed. The root account should never be used on these systems.
references	
tags	attack.t1098.004
logsource	product: Cisco SD-WAN service: System (auth) category: auth paths: /var/log/auth.log
detection	Search auth logs for 'Accepted publickey for root' entries; pivot to root's authorised_keys and session artefacts.
conditions	• message contains 'Accepted publickey for root'
falsepositives	• None; root SSH should not be used on Cisco SD-WAN devices
level	high
analytic_validation	Confirm presence/changes in /home/root/.ssh/authorized_keys; corroborate with /etc/ssh/sshd_config 'PermitRootLogin yes'.
samples	`Accepted publickey for root from <IP> port <port>`
related	PERSISTENCE-T1098.004-PermitRootLogin-016, PERSISTENCE-T1098.004-RootDiskArtefacts-024

PERSISTENCE-T1098.004-vmanage-adminSSHAuthorizedKey-012b

title	Root SSH Public Key Accepted
id	PERSISTENCE-T1098.004-vmanage-adminSSHAuthorizedKey-013b
status	stable
description	Detects SSH authentication using a public key for the ‘vmanage-admin’ account. The account is used by the system, but a rogue ‘authorized_key’ for ‘vmanage-admin’ is added during every initial access exploit.
references	
tags	attack.t1098.004
logsource	product: Cisco SD-WAN service: System (disk) category: file paths: /home/vmanage-admin/.ssh/authorized_keys/
detection	Search path for authorized_keys that are not related to the vManage (manager) component
conditions	
falsepositives	• The vManage component uses SSH and NETCONF backed by authorized_keys legitimately to maintain the other components.
level	medium
analytic_validation	Confirm presence/changes in /home/vmanage-admin/.ssh/authorized_keys;
samples	
related	PERSISTENCE-T1098.004-RootDiskArtefacts-024

PERSISTENCE-T1078-RootOrRogueLogins-013

title	Root or Rogue User Interactive Sessions
id	PERSISTENCE-T1078-RootOrRogueLogins-014
status	stable

description	Detects interactive sessions for the 'root' account or actor-created local users via system-login-change/system-logout-change events. Root interactive login should not occur.
references	
tags	attack.t1078, attack.t1136.001
logsource	product: Cisco SD-WAN service: vSmart (controller) category: auth, application paths: /var/log/tmplog/vdebug
detection	Select 'system-login-change'/'system-logout-change' where user-name equals 'root' or matches known rogue/local user names from related detections.
conditions	• message contains 'system-login-change' OR 'system-logout-change' • user-name == 'root' OR user-name IN <suspect_users>
falsepositives	• None for root; verify rogue user names to avoid alerting on legitimate maintenance accounts
level	high
analytic_validation	Correlate to sshd_config changes and authorised_keys updates; verify session timing against other malicious activity.
samples	`[SYSMGR pid: 900] %Viptela-vsmart1-sysmgrd-6-INFO-1400002: Notification: system-login-change severity-level:minor host-name:""vsmart1"" system-ip:<IP> user-name:""root"" user-id:"` `[SYSMGR pid: 900] %Viptela-vsmart1-sysmgrd-6-INFO-1400002: Notification: system-logout-change severity-level:minor host-name:""vsmart1"" system-ip:<IP> user-name:""root"" user-id:"`
related	PERSISTENCE-T1098.004-PermitRootLogin-016, PERSISTENCE-T1136.001-UserAddAAA-015

PERSISTENCE-T1136.001-UserAddAAA-014

title	**Suspicious Local User Create/AAA Changes**
id	PERSISTENCE-T1136.001-UserAddAAA-015
status	experimental

description	Detects creation or modification of local users and AAA properties (e.g., '/usr/sbin/useradd', 'cfgmgr_config_aaa_user') often around reboot/version-change windows.
references	
tags	attack.t1136.001
logsource	product: Cisco SD-WAN service: vSmart (controller) category: application paths: /var/log/tmplog/vdebug
detection	Select entries invoking '/usr/sbin/useradd' or 'cfgmgr_config_aaa_user'; inspect failures indicating user already exists; pivot on timestamps around reboots.
conditions	• message contains '/usr/sbin/useradd' • message contains 'cfgmgr_config_aaa_user'
falsepositives	• Legitimate user provisioning; baseline required
level	medium
analytic_validation	Cross-check with account inventory; correlate to downgrade/reversion windows.
samples	`[CFGMGR pid: 2965] vip_execute_handle_parent[123]: [/usr/sbin/useradd <user> -N -m -K UMASK=0077 -s /usr/sbin/viptela_cli] exited with ret: 9 output: useradd: user '<user>' already exists` `[CFGMGR pid: 2965] cfgmgr_config_aaa_user[2043]: Set (add) authtype to ssh failed for user: <user>` `[CFGMGR pid: 2965] cfgmgr_config_aaa_user[2089]: username <user> group basic`
related	PERSISTENCE-T1078-RootOrRogueLogins-014, PERSISTENCE-T1098.004-RootDiskArtefacts-024

PERSISTENCE-T1098.004-PermitRootLogin-015

title	**SSHD PermitRootLogin Enabled**
id	PERSISTENCE-T1098.004-PermitRootLogin-016
status	stable

description	Detects modification of '/etc/ssh/sshd_config' enabling 'PermitRootLogin yes', often accompanied by root SSH activity and creation of '/home/root/.ssh/'.
references	
tags	attack.t1098.004
logsource	product: Cisco SD-WAN service: System (disk) category: file paths: /etc/ssh/sshd_config, /home/root/.ssh/authorized_keys, /home/<user>/.ssh/known_hosts
detection	Check sshd_config for 'PermitRootLogin yes'; corroborate with presence of '/home/root/.ssh/', non-zero 'authorized_keys', and activity in auth/vdebug logs.
conditions	• file '/etc/ssh/sshd_config' contains 'PermitRootLogin yes' • exists '/home/root/.ssh/' • size('/home/root/.ssh/authorized_keys') > 0
falsepositives	• None expected in production configurations
level	critical
analytic_validation	Validate subsequent root SSH sessions and timeline of file creation vs activity logs; compare to peer vSmart for asymmetry.
samples	PermitRootLogin yes
related	PERSISTENCE-T1098.004-RootSSHKeyAccepted-013, PERSISTENCE-T1098.004-RootDiskArtefacts-024

LATERALMOVE-T1021.004-KnownHosts-016

title	**Anomalous Known Hosts (Root/Peer)**
id	LATERALMOVE-T1021.004-KnownHosts-017
status	experimental
description	Detects lateral movement indicators via SSH known_hosts entries, especially within '/home/root/.ssh/known_hosts' or unusual user known_hosts files.
references	
tags	attack.t1021.004

logsource	product: Cisco SD-WAN service: System (disk) category: file paths: /home/<user>/.ssh/known_hosts, /home/root/.ssh/known_hosts
detection	Identify new internal device keys in root's known_hosts; pivot by timestamps to reconstruct SSH connections.
conditions	• file '/home/root/.ssh/known_hosts' exists and contains internal addresses • file '/home/<user>/.ssh/known_hosts' contains vSmart root public key
falsepositives	• SSH by an interactive user to other systems, but this should be rare. • SSH from root should not occur
level	high
analytic_validation	Align creation/modification times with suspected activity; confirm corresponding SSH auth logs.
samples	known_hosts entries referencing internal devices on vManage and vSmart
related	PERSISTENCE-T1098.004-PermitRootLogin-016, PERSISTENCE-T1098.004-RootSSHKeyAccepted-013

PERSISTENCE-T1136.001-RollbackUserOps-017

title	**Rollback Files Indicate Rogue User Creation/Deletion**
id	PERSISTENCE-T1136.001-RollbackUserOps-018
status	experimental
description	Detects local user creation/deletion through configuration rollback files across '/var/confd/rollback', '/backup/rollback', '/var/ncs/rollback'.
references	
tags	attack.t1136.001
logsource	product: Cisco SD-WAN service: System (disk) category: file paths: /var/confd/rollback, /backup/rollback, /var/ncs/rollback

detection	Parse rollback deltas for 'system/aaa/user <name>' additions or 'delete: user <name>' operations; flag 'admin-local' creation as suspected persistence.
conditions	• rollback content contains 'system { aaa { user ' • rollback content contains 'delete: user '
falsepositives	• Legitimate account lifecycle changes; confirm with change records
level	medium
analytic_validation	Validate operator approvals; correlate with login events and ssh artefacts.
samples	`# User Creation` `system {` `  aaa {` `  user admin-local {` `  password <hash>;` `  group  [ basic ];` `  }` `  }` `}` `# User Deletion` `system {` `  aaa {` `  delete:` `  user admin-local;` `  }` `}`
related	PERSISTENCE-T1078-RootOrRogueLogins-014, PERSISTENCE-T1136.001-UserAddAAA-015

PRIVESC-T1601.002-RollbackCounterReset-018

title	**Rollback Sequence Counter Reset After Version Change**

id	PRIVESC-T1601.002-RollbackCounterReset-019
status	test
description	Identifies anomalies in rollback file sequence number and 'transactionid' counters (e.g., reset to 10001)
references	
tags	attack.t1601.002
logsource	product: Cisco SD-WAN service: System (disk) category: file paths: /var/confd/rollback, /backup/rollback, /var/ncs/rollback
detection	Sort rollback files by number and timestamp; flag transactionid counter resets in the
conditions	• sequence anomaly: rollback number resets to 10001 • transactionid decreases across successive files
falsepositives	• System maintenance that resets counters; verify against approved change records
level	low
analytic_validation	Use as a pointer to find missing logs of version changes; not reliable to attribute malicious changes alone.
samples	In the example below, both `36` and `35` rollback files are malicious: `38 rollback38 vmanage-admin <redacted>-06:32:31+00:00 netconf delta 10141 1398719` `37 rollback37 vmanage-admin <redacted>-06:42:37+00:00 netconf delta 10142 1398739` *`36 rollback36 vmanage-admin <redacted>-04:04:46+00:00 netconf delta 10143 1460328`* *`35 rollback35 vmanage-admin <redacted>-05:01:05+00:00 netconf delta 10001 1465999`*

	34 rollback34 vmanage-admin <redacted>-09:36:50+00:00 netconf delta 10002 1468570 33 rollback33 system-vdaemon <redacted>-09:39:20+00:00 system delta 10003 1468578 32 rollback32 vmanage-admin <redacted>-00:30:22+00:00 netconf delta 10004 1494133 31 rollback31 system-vdaemon <redacted>-00:32:52+00:00 system delta 10005 1494140
related	PRIVESC-T1601.002-AppDowngrade-001, PRIVESC-T1601.002-AppReversion-002

DEFENSEEVASION-T1070.003-BashVsCliHistory-019

title	**Bash vs CLI History Anomaly**
id	DEFENSEEVASION-T1070.003-BashVsCliHistory-020
status	experimental
description	Detects presence and timing of '~/.bash_history' vs encrypted 'cli-history' suggesting interactive bash use by compromised accounts; actor may not always clear bash history.
references	
tags	attack.t1070.003
logsource	product: Cisco SD-WAN service: System (disk) category: file paths: /var/confd/state/cli-history/<user>, /home/<user>/.bash_history
detection	Identify users with both cli-history (encrypted) and bash_history files where timestamps align with suspicious activity windows.
conditions	• exists '/home/<user>/.bash_history' • mtime(cli-history) ~ mtime(bash_history)
falsepositives	• Legitimate shell access by support under documented procedures

level	medium
analytic_validation	Compare 'stat' outputs; if bash history exists for root or unexpected users, escalate.
samples	`$ stat /var/confd/state/cli-history/<user>` `$ stat /home/<user>/.bash_history`
related	DEFENSEEVASION-T1070.003-ClearShellHistory-023, PERSISTENCE-T1098.004-RootDiskArtefacts-024

DEFENSEEVASION-T1070.002-ClearLoginLogs-020

title	**Clearing System Login Logs (wtmp/lastlog)**
id	DEFENSEEVASION-T1070.002-ClearLoginLogs-021
status	stable
description	Detects clearing of system login logs via redirection of /dev/null into 'wtmp' and 'lastlog', resulting in zero-byte files; triage with 'last' output.
references	
tags	attack.t1070.002
logsource	product: Cisco SD-WAN service: System (shell/disk) category: file, process paths: /var/log/lastlog, /var/log/wtmp
detection	Identify command history showing 'cat /dev/null > wtmp|lastlog' and verify resulting file sizes are 0 bytes; run 'last' for evidence of wipe.
conditions	• bash history contains 'cat /dev/null > wtmp' OR 'cat /dev/null > lastlog' • size('/var/log/wtmp') == 0 OR size('/var/log/lastlog') == 0
falsepositives	• Intentional log truncation during approved maintenance (rare)
level	high
analytic_validation	Run 'last' to confirm absence of historical sessions; inspect surrounding artefacts for root activity.
samples	`$ cat /dev/null > wtmp`

	$ cat /dev/null > lastlog $ last
related	DEFENSEEVASION-T1070.003-ClearShellHistory-023, PERSISTENCE-T1098.004-RootDiskArtefacts-024

DEFENSEEVASION-T1070.007-SearchRogueIP-021

title	**Searching Local Logs for Rogue VPN512 IP**
id	DEFENSEEVASION-T1070.007-SearchRogueIP-022
status	experimental
description	Detects actor behaviour grepping for the rogue peer's internal VPN512 IP across /var/log to identify and scrub evidence.
references	
tags	attack.t1070.007
logsource	product: Cisco SD-WAN service: System (shell) category: process paths: /var/log, ~/.bash_history
detection	Find bash history entries like 'grep -F <rogue VPN512 IP> * -l' executed under root in /var/log.
conditions	• bash history contains 'grep -F <rogue peer VPN512 IP address> * -l'
falsepositives	• Legitimate operator searches; verify IP ownership
level	high
analytic_validation	Confirm that the searched IP corresponds to observed rogue peer internal address (not public IP).
samples	$ cd /var/log $ grep –F <rogue peer VPN512 IP address> * -l
related	DEFENSEEVASION-T1070.002-ClearLoginLogs-021, DEFENSEEVASION-T1070.003-ClearShellHistory-023

DEFENSEEVASION-T1070.003-ClearShellHistory-022

title	Clearing Shell History
id	DEFENSEEVASION-T1070.003-ClearShellHistory-023
status	experimental
description	Detects clearing of '~/.bash_history' yielding 0/1/2-byte files via 'cat /dev/null' or 'echo' techniques; align timestamps with malicious windows.
references	
tags	attack.t1070.003
logsource	product: Cisco SD-WAN service: System (disk) category: file paths: /home/<user>/.bash_history
detection	Flag users whose bash_history size is 0 bytes (cat /dev/null), 1 byte (LF only), or 2 bytes (space+LF) post-activity.
conditions	• size('~/.bash_history') in {0,1,2}
falsepositives	• Fresh accounts that never executed commands (rare)
level	medium
analytic_validation	Correlate with CLI activity timestamps and other root/rogue artefacts.
samples	• `echo "" > .bash_history`, which will result in a 1 byte file containing a single Line Feed character (0x0a). • `cat /dev/null > .bash_history`, which will result in a 0 byte file. • `echo " " > .bash_history` which will result in a 2 byte file containing a space, and a Line Feed character (0x200a).
related	DEFENSEEVASION-T1070.002-ClearLoginLogs-021, PERSISTENCE-T1098.004-RootDiskArtefacts-024

PERSISTENCE-T1098.004-RootDiskArtefacts-023

title	Root Account Artefacts on Disk

id	PERSISTENCE-T1098.004-RootDiskArtefacts-024
status	stable
description	The `.bash_history` file is created in the user's home directory when the user logs in and executes commands in a bash shell for the first time and then closes that shell. In this case, the root user's `bash_history` file should not exist as the root user account is not generally used. In some cases, the file was also empty which would suggest that it was wiped, or that no commands were executed before the shell was terminated. In another file, it was observed that it contained the `/dev/null` command listed in the previous activity used to wipe the `wtmp` and `lastlog` files. The `known_hosts` file should also not exist as it is used for host authentication and security. It stores the public keys of remote servers that a user has previously connected to via SSH. Detects unexpected root shell artefacts: presence of '/home/root/.bash_history', non-zero '/home/root/.ssh/authorized_keys', and existence of '/home/root/.ssh/known_hosts'.
references	
tags	attack.t1098.004, attack.t1070.003
logsource	product: Cisco SD-WAN service: System (disk) category: file paths: /home/root/.bash_history, /home/root/.ssh/authorized_keys, /home/root/.ssh/known_hosts
detection	Alert if any of the above files exist in states that deviate from policy (should not exist or should be empty).
conditions	• exists '/home/root/.bash_history' • size('/home/root/.ssh/authorized_keys') > 0 • exists '/home/root/.ssh/known_hosts'
falsepositives	• None; root should not be used interactively
level	high
analytic_validation	Compare file modified times; look for commands in root's bash_history; verify keys and remote hosts.
samples	`$ stat /home/<user>/.bash_history` `$ cat /home/<user>/.ssh/authorized_keys`

related	PERSISTENCE-T1098.004-PermitRootLogin-016, PERSISTENCE-T1098.004-RootSSHKeyAccepted-013

CREDENTIALACCESS-T1110-PamFaillock-024

title	PAM Faillock Files for New/Compromised Accounts
id	CREDENTIALACCESS-T1110-PamFaillock-025
status	experimental
description	Detects creation/modification of pam_faillock files per user under '/var/volatile/log/faillock/<user>' which include the connecting IP and indicate failed authentications.
references	
tags	attack.t1110, attack.t1078
logsource	product: Cisco SD-WAN service: System (disk) category: file paths: /var/volatile/log/faillock/<user>
detection	Monitor for new/updated faillock files for newly created or abused accounts; extract IPs and correlate with activity.
conditions	• exists '/var/volatile/log/faillock/<user>' • mtime of faillock aligns with user creation or abuse
falsepositives	• Legitimate failed logins during password resets or onboarding
level	medium
analytic_validation	Use 'stat' and 'cat' to review timestamps and IPs; correlate with login failures and suspicious sessions.
samples	`$ stat /var/volatile/log/faillock/<user>` `$ cat /var/volatile/log/faillock/<user>`
related	PERSISTENCE-T1136.001-UserAddAAA-015, PERSISTENCE-T1078-RootOrRogueLogins-014

Mitigations

The following mitigation actions are a subset of recommended actions organisations should take to improve resilience of their SD-WAN. These mitigations will also form part of remediating a compromised system.

Please follow the vendors' hardening guide as the primary source for securing the SD-WAN.

Use the "Golden Star" SD-WAN Version

Use Cisco's recommended "golden star" software version. This ensures that the SD-WAN can implement the most current security features.

Patch the SD-WAN

Organisations should patch SD-WAN products as soon as practical to limit the opportunity for compromise.

Network Filtering

Use a firewall to only allow legitimate edge devices on the SD-WAN. Whilst this can be difficult, as certain carriers use dynamic IP ranges, it will minimise opportunity for discovery and exploitation.

Device Management interfaces should not be exposed to the internet and should be filtered to only allow legitimate admin IPs (e.g., jump boxes).

Data Plane Security

Configure the data plane to use pairwise key exchange to establish encrypted IPsec connections.

Centralised Logging

Ensure that logging is enabled on the SD-WAN products, particularly covering logs referenced in the hunt guide.

Logging must be centralised off the device to limit defense evasion.

Disclaimer

The information in this report is being provided “as is” for informational purposes only. Co-sealers do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by co-sealers.

Glossary

Term	Definition
PAM	Pluggable Authentication Module
SD-WAN	Software Defined Wide Area Network

Detection table standards

The following standards were used in the generation of the detection tables. This should allow some level of automation if desired.

title	Human-readable detection name (Sigma: `title`). Use Title Case, concise naming (e.g., *Application Downgrade*).
id	Unique ID for the detection. format: `<TACTIC>-<TECH>-<SHORT>-<SEQ>`
status	Optional Sigma field. Use: `stable`, `experimental`, or `test`. Default to experimental if unsure
description	A concise explanation of what the detection identifies and why it matters. Maps to Sigma `description`.
references	Any relevant links/urls
tags	ATT&CK technique IDs. Sigma uses `tags:` with `attack.t####` format.
logsource	Where logs originate (Sigma: `logsource`). Include product, service, category.
detection	Core detection logic—conditions, sequences, patterns (Sigma: `detection`).
conditions	In Sigma, this is part of `detection`. For your use, these correspond to specific patterns (e.g., `peer-type:vhub`).
falsepositives	Conditions that may trigger benign matches. Maps directly to Sigma `falsepositives`.
level	Sigma severity level: `low`, `medium`, `high`, `critical`.
analytic_validation	Not a Sigma field but allowed as custom metadata
samples	Not Sigma core but widely included as `samples:` or `examples:`. Provide at least two representative log lines—full, not truncated.
related	Internal links to other ACT-X.Y detections. Sigma supports custom metadata extensions (YAML) like `related:`.

Traffic Light Protocol

Alert classification	Restriction on access and use
RED	**Highly restricted** **Access to and use by your Australian Signals Directorate's Australian (ASD) Cyber Security Centre (ACSC) contact officer(s) only.** Information provided at **RED** contains information that cannot be effectively acted upon without significant risk for the privacy, reputation, or operations to the organisations involved. You must ensure that your ASD's contact officer(s) does not disseminate or discuss **RED** alerts with any other person, and you shall ensure that you have appropriate systems in place to ensure that the information cannot be accessed or used by any person other than your ASD's contact officer(s).
AMBER	**Limited disclosure** Information within **AMBER** alerts can only be shared with recipients on a 'needs-to-know' basis within your organisation, its clients, and/or service providers where the information is necessary to assist in the protection of your information and communications technology (ICT) systems. Note that **AMBER:STRICT** advice is restricted to your organisation ONLY.
GREEN	**Restricted to closed groups and subject to confidentiality** You may share **GREEN** alerts with external organisations, information exchanges or individuals in the network security, information assurance or critical network infrastructure community that agree to maintain the confidentiality of the information in the alert. You may not publish or post online or otherwise release it in circumstances where confidentiality may not be maintained.
CLEAR	**Not restricted** **CLEAR** alerts are not confidential. They contain information that is for public, unrestricted dissemination, publication, web-posting or broadcast. You may publish the information, subject to copyright and any restrictions or rights noted in the information.
Not classified	Any information received from ASD that is not classified in accordance with the Traffic light protocol must be treated as **AMBER** classified unless otherwise agreed in writing by ASD.

ASD adheres to the FIRST definitions of TLP, further information can be obtained at https://www.first.org/tlp

Russell Offices

51 Russell Dr

PO Box 5076, Kingston ACT 2604

A S D . G O V . A U