T1072 5G Orchestration and Deployment Tools

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
| 7/20 | Mudddasar | Impl-Virtualization, Supply-chain | Impl-OA&M, Impl-Virtualization, Supply-chain, RAN, UE | Impl-OA&M, Impl-Virtualization, Supply-chain, RAN, UE |
|  |  |  |  |  |

Description: An adversary may use CI/CD tools to gain access to production hosts/VNFs for discovery, data exfiltration and for deployment of lateral movements tools.

In 5G deployments, MNO’s development and deployment tools offer a conduit to 5G production RAN and Core network functions. CI/CD tools have a greater access to Software during development lifecycle, an adversary may be able to find a back door to software in production environment- a very similar scenario to SolarWinds hack, where compromised software was deployed on thousands of hosts via a software upgrade carrying compromised image.

Management and Orchestration is a framework for managing and orchestrating network functions virtualization (NFV) infrastructure, resources, and services. It provides a standard approach for the management and orchestration of network services in NFV environments, including the automation of tasks such as network service deployment, scaling, and network function lifecycle management. MANO toolset if misconfigured or APIs not properly secured can provide an attack vector to adversary with grave consequences to network and its services.

Labelling:

* Sub-techniques: none
* Applicable Tactics: Execution, Lateral Movement

Metadata:

* Architecture Segment: Impl-OA&M, Impl-Virtualization, Supply-chain, RAN, UE
* Platform(s): Infrastructure, PNF, VNF Hosts,
* Access type required: User/NPE/Administrative access
* Data Sources:
* Theoretical/Proof of concept/Observed:

Procedure Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| [G0091](https://attack.mitre.org/groups/G0091) | Silence has used RAdmin, a remote software tool used to remotely control workstations and ATMs |
| [S0041](https://attack.mitre.org/software/S0041) | It is believed that a patch management system for an anti-virus product commonly installed among targeted companies was used to distribute the Wiper malware |

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| M1018 | User Account Management, limited and least privileged user accounts |
| M1051 | Update Software regularly to eliminate persistence |
| M1029 | Remote Data Storage, restrict access and monitor repository activity |
| M1026 | Privileged Account Management, unique, least privileged accounts and regularly audit access attempts audits |
| M1027 | Password Policies, no credential sharing, create traceability |
| M1030 | Network Segmentation allows limit movements, insert application aware firewalls between segments |
| M1032 | Multi-factor Authentication adds additional layer of security for compromised credentials as well as increased accountability |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| CI/CD Tools | Software development and deployment tools in MNO (and supplier) environments |
| Security Tools | Scanning, monitoring, and end point protection tools |
| OSS Tools | Operation and system support tools |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| DS0015 | Often these third-party applications will have logs of their own that can be collected and correlated with other data from the environment. Ensure that third-party application logs are on-boarded to the enterprise logging system and the logs are regularly reviewed. Audit software deployment logs and look for suspicious or unauthorized activity. A system not typically used to push software to clients that suddenly is used for such a task outside of a known admin function may be suspicious. Monitor account login activity on these applications to detect suspicious/abnormal usage. Perform application deployment at regular times so that irregular deployment activity stands out. |
| DS0009 | Monitor for newly executed processes that does not correlate to known good software. Analyze the process execution trees, historical activities from the third-party application (such as what types of files are usually pushed), and the resulting activities or events from the file/binary/script pushed to systems. |
|  |  |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

References:

|  |  |
| --- | --- |
| Name | URL |
| ETSI NFV SEC001, “Network Functions Virtualization (NFV); NFV Security; Problem Statement”, Jan. 2014, section 6.9 | https://www.etsi.org/deliver/etsi\_gs/nfv-sec/001\_099/001/01.01.01\_60/gs\_nfv-sec001v010101p.pdf |
| R. Pell, S. Moschoyiannis, E. Panaousis, R. Heartfield, “Towards dynamic threat modelling in 5G core networks based on MITRE ATT&CK”,  October 2021 | https://arxiv.org/abs/2108.11206 |
| Dell SecureWorks. (2013, March 21). Wiper Malware Analysis Attacking Korean Financial Sector. Retrieved May 13, 2015. | http://www.secureworks.com/cyber-threat-intelligence/threats/wiper-malware-analysis-attacking-korean-financial-sector/ |
| Silence – a new Trojan attacking financial organizations ( accessed 06/20/2023 | https://securelist.com/the-silence/83009/ |