Root Cause Analysis (RCA) Report: CVE-2019-0708 Evasion Coverage Incident

Summary of Incident

On May 25th, Cisco TAC began to receive calls from customers indicating their legitimate RDP traffic was being dropped by SIDs 50186-50189. TAC escalated to Talos at 8:36 am, and by 9:25 am EDT, TAC was advised to recommend customers disable these SIDs as a return-to-service remedy. Eventually, 72 escalations were opened with Cisco TAC for this issue. The incident was also escalated within Talos to the Detection Response Team. After quick analysis of the situation, Talos leadership decided to build and deploy an SRU with SIDs 50186-50189 deleted, and to withdraw the SRU which had contained them.

A new build was initiated at 12:04 pm EDT, and updated releases were available by 3:37 pm EDT. The SRU including the problematic SIDs was removed from the Cisco download site by 7:18 pm May 25th.

Incident Categorization

Incident Date: 5/24/2019 - 5/25/2019
Incident Type: False Positive IPS Block
Severity Level: P1

Incident Timeline

Time (PDT)	Details
8:36 AM EDT	TAC escalates the incident to Talos Escalations
9:25 AM EDT	Talos Escalations advises TAC to recommend to the customer disabling SIDs 50186-50189
12:04 PM EDT	New SRU build initiated.
3:37 PM EDT	New SRU without SIDs 50186-50189 available to customers
3:53 PM EDT	TAC informed that a new SRU was available on the Cisco download site
7:18 PM EDT	SRU containing SIDs 50186-50189 removed from the Cisco download site

Root Cause

On May 14, 2019 Microsoft released fixes for a critical pre-authentication remote code execution vulnerability (CVE-2019-0708 a.k.a. "BlueKeep") in Remote Desktop Protocol Services (RDP). SID 50137 was released on May 20th 2019, providing an IPS rule which would interrupt the identified attack vector for CVE-2019-0708.

After SID 50137 was released on May 20th, 2019, further research showed a possible evasion that an attacker could use to blind the Firepower product from seeing the vulnerable condition blocked by SID 50137. Namely, attackers could craft a request that would require the connection be encrypted immediately thereby preventing the Firepower product from stopping the exploit in transit. Telemetry indicated that attackers may already be scanning for vulnerable RDP servers that allow this type of early encryption.

Rules were written (SIDs 50186-50189) to rewrite the RDP requested protocols such that attackers would only have two options when interacting with RDP servers behind Firepower NGFWs: 1.) Authenticate with the RDP server using Network Level Authentication (NLA). 2.) Use legacy RDP session setup thereby requiring exploitation attempts be sent in the clear allowing us to block them. If no exploitation attempt was found, legacy RDP session setup would proceed to encrypt the connection.

SIDs 50186-50189 were tested on multiple Cisco Firepower Next Generation Firewalls in the Talos lab and RDP sessions were shown to connect and proceed normally with the rules active. However, this does not agree with what our customers experienced, nor with our post-mortem analysis of customer PCAPs in the following days. In retrospect, not enough scenarios were tested in the lab. For example: extended network level authentication was not tested. The wide range of RDP clients and servers available also made exhaustive testing difficult.

Talos SRUs are subjected to an extensive pre-release validation process, including deployment on all supported versions of the Firepower product and deployment to devices in Talos' Crete program. No errors or false positives were observed during this process for the SRU released on May 24th that contained SIDs 50186-50189.

Re-writing network traffic is a technique that is used, as a rule, only in extreme circumstances. It was attempted here as an aggressive attempt to defend our customers against an exploit with huge potential for damage, and it failed.

Corrective Actions

We understand that such incidents have a negative impact on the business of our customers, and we are committed to constantly improve customer experience. To prevent the re-occurrence of this issue, we have planned or have implemented the following corrective actions:

Item#	Category	Description	Status
1	FP Mitigation	Customers advised to disable SIDs 50186-50189	Completed
2	FP Mitigation	An SRU was deployed with SIDs 50186-50189 deleted, and the SRU including those SIDs was removed from the download site	Completed
For any future intrusion prevention strategy employing the re-writing of network traffic:			
3	Process Change	More extensive testing will be required	Planned

4	Process Change	Additional technical reviewers’ concurrence will be required before release	Planned
5	Process Change	Senior management approval will be required before release	Planned