Title: RSA NetWitness Endpoint 4.x Windows Agent Technical Advisory

Summary: Due to recent changes in the Windows 10, version 1903 kernel, NetWitness Endpoint (NWE) 4.x agents may have received content which could cause agent systems to encounter a system stop error (aka. BSOD). Steps need to be taken to resolve and avoid this issue in customer environments.

Affected Products: NWE 4.x agents running on Windows 10 version 1903

Impact: agent systems running Windows 10 build 1903 may encounter a system stop error (aka. BSOD). NWE servers receive kernel encoding content from RSA Live. Agents receive kernel encodings from NWE servers. Updated Windows 10 version 1903 kernel encodings were published to RSA Live to correct the issue and need to be updated in the NWE server database as well as on agents running on the affected Windows version.

Solution: To update deployed NWE servers and agents, perform following steps:

On each NWE server:

1. Stop the RSA ECAT Server service.
2. In SQL Management Studio, run the following command for each ECAT$PRIMARY and ECAT$SECONDARY database:
   `delete KernelData where Description like '10.0.18362.%'`
3. Run the following SQL command and confirm that old kernel encodings were deleted:
   `select * from KernelData where Description like '10.0.18362.%'`
   There should be 0 active encodings at this time.
4. Restart the RSA ECAT Server service.
   Note: Updated content should be downloaded automatically by NWE servers from RSA Live within 30 minutes.
5. Confirm the content update by running the following command:
   `select * from KernelData where Description like '10.0.18362.%'`

In environments without direct access to RSA Live, use the `ConsoleServerSync` utility to update kernel data. Perform the following steps for all agents running Windows 10 build 1903:

1. Upgrade or re-install agents running on Windows 10 version 1903 systems.
2. If you are re-installing agents use, the Force Overwrite option in NetWitness Endpoint Packager.

Agents will download and use updated content from NWE servers.

EOPS Policy: RSA has a defined End of Primary Support policy associated with all major versions. Please refer to Product Version Life Cycle for additional details.