Dell Client Statement on Intel AMT Advisory (INTEL-SA-00075)

UPDATED: June 15, 2017

NOTE: Dell PowerEdge systems are detailed in a separate response that you can find at the link below: http://en.community.dell.com/techcenter/extras/m/white_papers/20443937

References

Intel Security Advisory (INTEL-SA-00075):
https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr
Intel Mitigation Guide - https://downloadcenter.intel.com/download/26754
Intel Detection Guide and Discovery Tool - https://downloadcenter.intel.com/download/26755
Intel Unprovisioning Tool - https://downloadcenter.intel.com/download/26781
CVE-2017-5689 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5689
CERT VU#491375 - https://www.kb.cert.org/vuls/id/491375
CERT VU#491375 (Dell) - https://www.kb.cert.org/vuls/id/BLUU-ALYSH5

Overview

Dell is aware of the industry-wide vulnerability described in the Intel Security Center advisory INTEL-SA-00075 that can affect Dell business PCs that support system manageability via Intel Active Management Technology (AMT), Intel Small Business Technology (SBT), or Intel Standard Manageability (ISM). We are diligently working on helping our customers mitigate the vulnerability through BIOS firmware updates for impacted Dell business products. The firmware update details for these Dell business PCs will be added to this document as they become available.

Recommendation

Dell recommends customers follow the Intel published Detection Guide and Mitigation Guide for these systems immediately. Intel has released a Discovery Tool that can be used by local users or IT administrators to determine whether a system is vulnerable to INTEL-SA-00075. The Mitigation Guide includes instructions and an Unprovisioning Tool to unprovision manageability on affected systems.

Customers should update to the latest BIOS by downloading the patched releases from http://support.dell.com as those releases become available.

BIOS Release Details

The systems below are affected and will receive patched Intel firmware via Dell BIOS updates as they become available. This list of systems represents a superset of all possible affected products *but only those purchased with Intel AMT, SBT, or ISM capability are vulnerable*. This list is provided for customer planning purposes and will be updated with release information when available:

Dell Client System	Patched Firmware	BIOS Update
OptiPlex 7050	11.6.29.3287	1.3.11
OptiPlex 5050	11.6.29.3287	1.3.11
OptiPlex 7450 AIO	11.6.29.3287	1.3.6
OptiPlex 5250 AIO	11.6.29.3287	1.3.6
OptiPlex 7040	11.0.26.3000	1.5.10
OptiPlex 5040	11.0.26.3000	1.5.10
OptiPlex 7440 AIO	11.0.26.3000	1.8.0
OptiPlex XE2	9.1.41.3024	A19
Latitude 5580	11.6.29.3287	1.3.3
Latitude 5480	11.6.29.3287	1.3.3
Latitude 5280	11.6.29.3287	1.3.3
Latitude 7280	11.6.29.3287	1.3.3
Latitude 7480	11.6.29.3287	1.3.3
Latitude 5289	11.6.29.3287	1.4.0
Latitude 5285	11.6.29.3287	1.1.6
Latitude E5270	11.0.26.3000	1.14.4
Latitude E5470	11.0.26.3000	1.14.4
Latitude E5570	11.0.26.3000	1.14.4
Latitude E7270	11.0.26.3000	1.15.4
Latitude E7270 Mobile Thin Client	11.0.26.3000	1.15.4
Latitude E7470	11.0.26.3000	1.15.4
Latitude 7275	11.0.25.3001	1.1.31
Latitude 7370	11.0.25.3001	1.12.4
Latitude 5179	11.0.25.3001	1.0.24
Latitude 5175	11.0.25.3001	1.0.24
Precision 3620	11.6.29.3287	2.3.0
Precision 3420	11.6.29.3287	2.3.0
Precision 5720 AIO	11.6.29.3287	2.2.0
Precision 5520	11.6.29.3287	1.3.3
Precision 7520	11.6.29.3287	1.4.1
Precision 7720	11.6.29.3287	1.4.1
Precision 3520	11.6.29.3287	1.3.3
Precision 3510	11.0.26.3000	1.14.4

Precision 5510	11.0.26.3000	1.2.25
Precision 7510	11.0.26.3000	1.12.4
Precision 7710	11.0.26.3000	1.12.4
Precision T5810	9.1.41.3024 (WS)	A19
Precision T7810	9.1.41.3024 (WS)	A19
Precision T7910	9.1.41.3024 (WS)	A19
XPS 9365	11.6.29.3287	1.0.15
XPS 9360	11.6.29.3287	1.3.5
Latitude 7202	10.0.55.3000	A14
Latitude 7214	11.0.25.3001	1.11.0
Latitude 5414	11.0.25.3001	1.11.0
Latitude 7414	11.0.25.3001	1.11.0
Wyse 7040 Thin Client	11.0.26.3000	1.5.0
OptiPlex 9020M	9.1.41.3024	A13
OptiPlex 9020 Wyse Edition	9.1.41.3024	A13
OptiPlex 9030 AIO	9.1.41.3024	A16
OptiPlex 7020	9.1.41.3024	A12
OptiPlex 9020	9.1.41.3024	A19
OptiPlex 9020 AIO	9.1.41.3024	A15
OptiPlex 7010	8.1.71.3608	A25
OptiPlex 9010 AIO	8.1.71.3608	A20
OptiPlex 9010	8.1.71.3608	A26
OptiPlex 790	7.1.91.3272	A19
OptiPlex 990	7.1.91.3272	A20
OptiPlex 980	6.2.61.3535	A17
Latitude 7350	10.0.55.3000	A12
Latitude 7140	10.0.55.3000	A12
Latitude E7250	10.0.55.3000	A16
Latitude E7450	10.0.55.3000	A16
Latitude E5250	10.0.55.3000	A15
Latitude E5450	10.0.55.3000	A15
Latitude E5550	10.0.55.3000	A15
Latitude E6440	9.1.41.3024	A17
Latitude E6440 ATG	9.1.41.3024	A17
Latitude E6540	9.1.41.3024	A20
Latitude E7240	9.5.61.3012	A21
Latitude E7440	9.5.61.3012	A21
Latitude E5440	9.5.61.3012	A18
Latitude E5540	9.5.61.3012	A18
Venue 11 Pro 7130	9.5.61.3012	A23
Latitude E6230	8.1.71.3608	A18
Latitude E6330	8.1.71.3608	A19

Latitude E6430	8.1.71.3608	A21
Latitude E6430 ATG	8.1.71.3608	A21
Latitude E6430S	8.1.71.3608	A19
Latitude E6530	8.1.71.3608	A20
Latitude E6430U	8.1.71.3608	A13
Latitude E5430	8.1.71.3608	A19
Latitude E5530	8.1.71.3608	A20
Latitude E6320	7.1.91.3272	A20
Latitude E6420	7.1.91.3272	A24
Latitude E6420 ATG	7.1.91.3272	A24
Latitude E6520	7.1.91.3272	A20
Latitude E6420 XFR	7.1.91.3272	A24
Latitude E6220	7.1.91.3272	A14
Latitude XT3	7.1.91.3272	A14
Latitude E4310	6.2.61.3535	A15
Latitude E6510	6.2.61.3535	A17
Latitude E6410	6.2.61.3535	A17
Latitude E6410 ATG	6.2.61.3535	A17
Latitude 7204	9.5.61.3012	A11
Latitude 7404	9.5.61.3012	A12
Latitude 5404	9.5.61.3012	A12
XPS 9350	11.0.26.3000	1.4.17
XPS 9343	10.0.55.3000	A12
Precision M4800	9.1.41.3024	A19
Precision M6800	9.1.41.3024	A19
Precision M2800	9.1.41.3024	A10
Precision T1700	9.1.41.3024	A22
Precision T3610	8.1.71.3608 (WS)	A14
Precision T5610	8.1.71.3608 (WS)	A14
Precision T7610	8.1.71.3608 (WS)	A14
Precision R7610	8.1.71.3608 (WS)	A13
Precision M4700	8.1.71.3608	A17
Precision M6700	8.1.71.3608	A18
Precision T1650	8.1.71.3608	A24
Precision M4600	7.1.91.3272	A17
Precision M6600	7.1.91.3272	A16
Precision T1600	7.1.91.3272	A17
Precision T7600	7.1.91.3272 (WS)	A13
Precision T5600	7.1.91.3272 (WS)	A15
Precision T5600XL	7.1.91.3272 (WS)	A15
Precision T3600	7.1.91.3272 (WS)	A15
Precision T3600XL	7.1.91.3272 (WS)	A15
Precision M4500	6.2.61.3535	A16

Acknowledgements

Dell would like to thank Maksim Malyutin from Embedi for reporting this vulnerability and working with Intel on coordinated disclosure.