باسمه‌تعالی

ROCA: حمله‌ی فاکتورگیری برای بازیابی کلیدهای خصوصی RSA

چکیده خبر

اگر فکر می‌کنید که حمله‌ی KRACK برای وای‌فای بدترین آسیب‌پذیری سال جاری است، پس این خبر را با دقت بخوانید...

آسیب‌پذیری دیگری وجود دارد که می‌تواند بدتر از حمله KRACK باشد. دیروز شرکت‌های مایکروسافت، گوگل، Lenovo، HP و فوجیتسو به مشتریان خود درباره‌ی یک آسیب‌پذیری جدی در کتابخانه‌ی رمزنگاری RSA هشدار دادند. برای بهره‌برداری از این آسیب‌پذیری فقط داشتن کلید عمومی ضروری است و نیازی به دسترسی فیزیکی به دستگاه آسیب‌پذیر نیست. این آسیب‌پذیری به مهاجم این امکان را می‌دهد که داده‌های حساس قربانی را رمزگشایی کند، کد مخرب به نرم‌افزار امضاء شده‌ی دیجیتالی تزریق کند و حفاظت‌هایی که مانع دسترسی یا سوءاستفاده از کامپیوتر هدف می‌شوند را دور بزند.

شرح خبر

این آسیب‌پذیری (CVE-2017-15361) مرتبط با رمزگذاری، مربوط به خود استاندارد رمزنگاری نبوده بلکه در پیاده‌سازی تولید جفت کلید RSA توسط TPM (Trusted Platform Module) اینفینئون (شرکت آلمانی تولیدکننده تجهیزات الکترونیکی و نیمه‌هادی‌ها) قرار دارد.

TPM یک میکروکنترلر اختصاصی است که به طور گسترده مورد استفاده قرار می‌گیرد و برای امن کردن سخت‌افزار از طریق ادغام کلید رمزنگاری در دستگاه‌ها طراحی شده و برای فرآیندهای رمزنگاری امن‌شده استفاده می‌شود.

این آسیب‌پذیری الگوریتمی سابقه ۵ ساله داشته و به تازگی توسط محققان امنیتی در دانشگاه ماساریک در جمهوری چک کشف شده است.

ROCA: حمله‌ی فاکتورگیری برای بازیابی کلیدهای خصوصی RSA

حمله‌ی فاکتورگیری ROCA (Return of Coppersmith's Attack) که توسط محققان معرفی شده است، به مهاجم راه دور این امکان را می‌دهد که فقط با داشتن کلید عمومی هدف، کلید خصوصی رمزنگاری را محاسبه کند.

برای اجرای حمله، فقط داشتن کلید عمومی ضروری است و نیازی به دسترسی فیزیکی به دستگاه آسیب‌پذیر نیست. این آسیب‌پذیری وابسته به تولیدکننده‌ی عدد تصادفی معیوب و ضعیف نبوده و همه‌ی کلیدهای RSA تولید شده تراشه‌ی آسیب‌پذیر در معرض خطر قرار دارند.

سوءاستفاده از این آسیب‌پذیری به مهاجم این امکان را می‌دهد که داده‌های حساس قربانی را رمزگشایی کند، کد مخرب به نرم‌افزار امضاء شده‌ی دیجیتالی تزریق کند و حفاظت‌هایی که مانع دسترسی یا سوءاستفاده از کامپیوتر هدف می‌شوند را دور بزند.

حمله‌ی ROCA میلیاردها دستگاه را در معرض خطر قرار می‌دهد

حمله‌ی ROCA بر روی تراشه‌های تولیدشده از اوایل سال ۲۰۱۲ توسط اینفینئون و برای تمامی طول‌های کلیدی از جمله ۱۰۲۴ و ۲۰۴۸ بیت که معمولاً در کارت‌های شناسایی ملی، مادربردهای PC برای ذخیره‌ی امن رمزهای عبور، در توکن‌های احراز اصالت، در طول مرور امن وب و برای حفاظت از پیام مانند PGP استفاده شده است، تاثیر می‌گذارد.

این آسیب‌پذیری امنیت کامپیوترهای دولتی و سازمانی محافظت‌شده با استفاده از تراشه‌ها و کتابخانه‌ی رمزنگاری اینفینئون را نیز تضعیف می‌کند.

اکثر دستگاه‌های ویندوزی و ChromeBook گوگل که توسط HP، Lenovo و Fujitso توسعه‌یافته‌اند، تحت تاثیر حمله‌ی ROCA قرار دارند.

تعداد کل کلیدهای آسیب‌پذیر تاییدشده تاکنون حدود ۷۶۰۰۰۰ است اما احتمالاً این تعداد دو تا سه برابر این مقدار است.

این آسیب‌پذیری در فوریه‌ی سال جاری به شرکت تکنولوژی‌های اینفینئون گزارش داده شد و محققان یافته‌های کامل خود را در تاریخ ۲ نوامبر در کنفرانس ACM در بخش امنیت ارتباطات و کامپیوتر ارائه دادند.

بنابراین شرکت سازنده زمان کافی برای تغییر کلیدهای رمزنگاری آسیب‌پذیر قبل از اینکه جزئیات نحوه‌ی کار آسیب‌پذیری و نحوه‌ی بهره‌برداری از آن منتشر شود، داشتند.

اکثر فروشندگان از جمله اینفینئون، مایکروسافت، گوگل، HP، لنوو و فوجیتسو به‌روزرسانی‌های نرم‌افزاری‌ای را برای سخت‌افزارها و نرم‌افزارهای مرتبط و همچنین دستورالعمل‌هایی را برای کاهش آسیب‌پذیری منتشر کرده‌اند. بنابراین به کاربران اکیداً توصیه می‌شود که دستگاه‌هایشان را هرچه زودتر وصله کنند.

فهرست تجهیزات آسیب‌پذیر

شرکت fujitsu

- TPM1.2 - FW133.32, FW149.32 (SLB9645)
- TPM1.2 - FW4.00 up to FW4.33 (SLB9655/9656)
- TPM1.2 - FW4.40 up to FW4.42 (SLB9660)
- TPM1.2 - FW6.00 up to FW6.42 (SLB9670)
- TPM2.0 - FW 5.00 up to FW5.61 (SLB9665)
- TPM2.0 - FW7.00 up to FW7.61 (SLB9670)

تجهیزات گوگل

- asuka - Dell Chromebook 13 3380
- auron-paine - Acer Chromebook 11 (C740)
- auron-yuna - Acer Chromebook 15 (CB5-571)
- banjo - Acer Chromebook 15 (CB3-531)
- banon - Acer Chromebook 15 (CB3-532)
- buddy - Acer Chromebase 24
- candy - Dell Chromebook 11 (3120)
- caroline - Samsung Chromebook Pro
- cave - ASUS Chromebook Flip C302
- celes - Samsung Chromebook 3
- chell - HP Chromebook 13 G1
- clapper - Lenovo N20 Chromebook
- cyan - Acer Chromebook R11 (CB5-132T / C738T)
- daisy-skate - HP Chromebook 11 2000-2099 / HP Chromebook 11 G2
- daisy-spring - HP Chromebook 11 1100-1199 / HP Chromebook 11 G1
- edgar - Acer Chromebook 14 (CB3-431)

- elm - Acer Chromebook R13 (CB5-312T)
- enguarde - ASI Chromebook
- enguarde - Crambo Chromebook
- enguarde - CTL N6 Education Chromebook
- enguarde - Education Chromebook
- enguarde - eduGear Chromebook R
- enguarde - Edxis Education Chromebook
- enguarde - JP Sa Couto Chromebook
- enguarde - Lenovo N21 Chromebook
- enguarde - M&A Chromebook
- enguarde - RGS Education Chromebook
- enguarde - Senkatel C1101 Chromebook
- enguarde - True IDC Chromebook
- enguarde - Videonet Chromebook
- expresso - Bobicus Chromebook 11
- expresso - Consumer Chromebook
- expresso - Edxis Chromebook
- expresso - HEXA Chromebook Pi
- falco - HP Chromebook 14
- gandof - Toshiba Chromebook 2 (2015 Edition)
- glimmer - Lenovo ThinkPad 11e Chromebook
- gnawty - Acer Chromebook 11 (C730 / C730E)
- gnawty - Acer Chromebook 11 (C735)
- guado - ASUS Chromebox CN62
- hana - Lenovo N23 Yoga/Flex 11 Chromebook
- hana - Poin2 Chromebook 14
- heli - Haier Chromebook 11 G2
- kefka - Dell Chromebook 11 Model 3180
- kefka - Dell Chromebook 11 3189
- kevin - Samsung Chromebook Plus
- kip - HP Chromebook 11 2100-2199 / HP Chromebook 11 G3
- kip - HP Chromebook 11 2200-2299 / HP Chromebook 11 G4/G4 EE
- kip - HP Chromebook 14 ak000-099 / HP Chromebook 14 G4
- lars - Acer Chromebook 11 (C771, C771T)
- lars - Acer Chromebook 14 for work (CP5-471)
- leon - Toshiba Chromebook
- link - Google Chromebook Pixel
- lulu - Dell Chromebook 13 7310
- mccloud - Acer Chromebox

- monroe - LG Chromebase 22CB25S
- monroe - LG Chromebase 22CV241
- ninja - AOPEN Chromebox Commercial
- nyan-big - Acer Chromebook 13 (CB5-311)
- nyan-blaze - HP Chromebook 14 x000-x999 / HP Chromebook 14 G3
- nyan-kitty - Acer Chromebase
- orco - Lenovo 100S Chromebook
- panther - ASUS Chromebox CN60
- peach-pi - Samsung Chromebook 2 13"
- peach-pit - Samsung Chromebook 2 11"
- peppy - Acer C720 Chromebook
- quawks - ASUS Chromebook C300
- reks - Lenovo N22 (Touch) Chromebook
- reks - Lenovo N23 Chromebook
- reks - Lenovo N23 Chromebook (Touch)
- reks - Lenovo N42 (Touch) Chromebook
- relm - Acer Chromebook 11 N7 (C731)
- relm - CTL NL61 Chromebook
- relm - Edxis Education Chromebook
- relm - HP Chromebook 11 G5 EE
- relm - Mecer V2 Chromebook
- rikku - Acer Chromebox CXI2
- samus - Google Chromebook Pixel (2015)
- sentry - Lenovo Thinkpad 13 Chromebook
- setzer - HP Chromebook 11 G5 / HP Chromebook 11-vxxx
- squawks - ASUS Chromebook C200
- sumo - AOpen Chromebase Commercial
- swanky - Toshiba Chromebook 2
- terra - ASUS Chromebook C202SA
- terra - ASUS Chromebook C300SA/C301SA
- tidus - Lenovo ThinkCentre Chromebox
- tricky - Dell Chromebox
- ultima - Lenovo ThinkPad 11e Chromebook 3rd Gen (Yoga/Clamshell)
- veyron-fievel - AOpen Chromebox Mini
- veyron-jaq - Haier Chromebook 11
- veyron-jaq - Medion Akoya S2013
- veyron-jaq - True IDC Chromebook 11
- veyron-jaq - Xolo Chromebook
- veyron-jerry - CTL J2 / J4 Chromebook for Education

- veyron-jerry - eduGear Chromebook K Series
- veyron-jerry - Epik 11.6" Chromebook ELB1101
- veyron-jerry - HiSense Chromebook 11
- veyron-jerry - Mecer Chromebook
- veyron-jerry - NComputing Chromebook CX100
- veyron-jerry - Poin2 Chromebook 11
- veyron-jerry - Positivo Chromebook CH1190
- veyron-jerry - VideoNet Chromebook BL10
- veyron-mickey - ASUS Chromebit CS10
- veyron-mighty - Chromebook PCM-116E
- veyron-mighty - eduGear Chromebook M Series
- veyron-mighty - Haier Chromebook 11e
- veyron-mighty - Lumos Education Chromebook
- veyron-mighty - MEDION Chromebook S2015
- veyron-mighty - Nexian Chromebook 11.6-inch
- veyron-mighty - Prowise 11.6" Entry Line Chromebook
- veyron-mighty - Sector 5 E1 Rugged Chromebook
- veyron-mighty - Viglen Chromebook 11
- veyron-minnie - ASUS Chromebook Flip C100PA
- veyron-speedy - ASUS Chromebook C201PA
- veyron-tiger - AOpen Chromebase Mini
- winky - Samsung Chromebook 2 11 - XE500C12
- wizpig - CTL J5 Chromebook
- wizpig - Edugear CMT Chromebook
- wizpig - Haier Convertible Chromebook 11 C
- wizpig - PCMerge Chromebook PCM-116T-432B
- wizpig - Prowise ProLine Chromebook
- wizpig - Viglen Chromebook 360
- wolf - Dell Chromebook 11
- zako - HP Chromebox CB1-(000-099) / HP Chromebox G1/ HP Chromebox for Meetings
- Chrome OS M61 - build 9765.81.0 and later
- Chrome OS M62 - build 9901.42.0 and later
- Chrome OS M63 - build 10020.0.0 and later

شرکت HP

- HP Chromebook 11 G4 EE
- HP Chromebook 11 G5

- HP Chromebook 11 G5 EE
- HP Chromebook 13 G1
- HP Chromebook 14 G4
- HP Elite x2 1011 G1 Tablet
- HP Elite x2 1012 G1 Tablet
- HP Elite x2 1012 G2 Tablet
- HP EliteBook 1020 G2
- HP EliteBook 1030 G1
- HP EliteBook 1040 G2
- HP EliteBook 1040 G3
- HP EliteBook 1040 G4
- HP EliteBook 612 G1
- HP EliteBook 720 G1
- HP EliteBook 720 G2
- HP EliteBook 725 G2
- HP EliteBook 725 G3
- HP EliteBook 725 G4
- HP EliteBook 740 G1
- HP EliteBook 740 G2
- HP EliteBook 745 G2
- HP EliteBook 745 G3
- HP EliteBook 745 G4
- HP EliteBook 750 G1
- HP EliteBook 750 G2
- HP EliteBook 755 G2
- HP EliteBook 755 G3
- HP EliteBook 755 G4
- HP EliteBook 820 G1
- HP EliteBook 820 G2
- HP EliteBook 820/828 G3
- HP EliteBook 820/828 G4
- HP EliteBook 840 G1
- HP EliteBook 840 G2
- HP EliteBook 840/848 G3
- HP EliteBook 840/848 G4
- HP EliteBook 850 G1
- HP EliteBook 850 G2

- HP EliteBook 850 G3
- HP EliteBook 850 G4
- HP EliteBook Folio 1040 G1
- HP EliteBook Folio 9480m
- HP EliteBook Folio G1
- HP EliteBook Revolve 810 G2
- HP EliteBook Revolve 810 G3
- HP EliteBook x360 1020 G2 Notebook PC
- HP EliteBook x360 G2
- HP ElitePad 1000 G2
- HP mt20 Mobile Thin Client
- HP mt21 Mobile Thin Client
- HP mt40 Mobile Thin Client
- HP mt41 Mobile Thin Client
- HP mt42 Mobile Thin Client
- HP mt43 Mobile Thin Client
- HP Pro Tablet 608 G1
- HP Pro x2 612 G2
- HP ProBook 11 G2
- HP ProBook 430 G1
- HP ProBook 430 G2
- HP ProBook 430 G3
- HP ProBook 430 G4
- HP ProBook 430 G5
- HP ProBook 440 G1
- HP ProBook 440 G2
- HP ProBook 440 G3
- HP ProBook 440 G4
- HP ProBook 440 G5
- HP ProBook 445 G1
- HP ProBook 445 G2
- HP ProBook 450 G1
- HP ProBook 450 G2
- HP ProBook 450 G3
- HP ProBook 450 G4
- HP ProBook 450 G5
- HP ProBook 455 G1

- HP ProBook 455 G2
- HP ProBook 455 G3
- HP ProBook 455 G4
- HP ProBook 470 G1
- HP ProBook 470 G2
- HP ProBook 470 G3
- HP ProBook 470 G4
- HP ProBook 470 G5
- HP ProBook 640 G1
- HP ProBook 640 G2
- HP ProBook 640 G3
- HP ProBook 645 G1
- HP ProBook 645 G2
- HP ProBook 645 G3
- HP ProBook 650 G1
- HP ProBook 650 G2
- HP ProBook 650 G3
- HP ProBook 650 G3
- HP ProBook 655 G2
- HP ProBook 655 G3
- HP ProBook x360 11 G1 EE
- HP ProBook x360 11 G2 EE
- HP Spectre Pro 13 G1
- HP Spectre Pro x360 G2
- HP Stream 11 Pro G2
- HP Stream 11 Pro G3
- HP Stream 11 Pro G4 EE
- HP Stream 14 Pro G3
- HP ZBook 14u G4 Mobile Workstation
- HP ZBook 15 Mobile Workstation
- HP ZBook 15 G2 Mobile Workstation
- HP ZBook 15 G3 Mobile Workstation
- HP ZBook 15 G4 Mobile Workstation
- HP ZBook 15u G3 Mobile Workstation
- HP ZBook 15u G4 Mobile Workstation
- HP ZBook 17 Mobile Workstation
- HP ZBook 17 G2 Mobile Workstation

- HP ZBook 17 G3 Mobile Workstation
- HP ZBook 17 G4 Mobile Workstation
- HP ZBook Studio G3 Mobile Workstation
- HP ZBook Studio G4 Mobile Workstation
- HP ZHAN 66 Pro G1
- HP 260 G1 Desktop Mini PC
- HP 260 G2 Desktop Mini PC
- HP 280 G1 MT Business PC
- HP 280 G2 MT Business PC
- HP 280 G2 MT Business PC
- HP 285 Pro G1 MT Business PC
- HP 285 Pro G2 MT Business PC
- HP 406 G1 MT Business PC
- HP 406 G2 MT Business PC
- HP Elite Slice
- HP EliteDesk 700 G1 Microtower PC
- HP EliteDesk 700 G1 Small Form Factor PC
- HP EliteDesk 705 G1 Desktop Mini PC
- HP EliteDesk 705 G1 Microtower PC
- HP EliteDesk 705 G1 Small Form Factor PC
- HP EliteDesk 705 G2 Desktop Mini PC
- HP EliteDesk 705 G2 Microtower PC
- HP EliteDesk 705 G2 Small Form Factor PC
- HP EliteDesk 705 G3 Desktop Mini PC
- HP EliteDesk 705 G3 Microtower PC
- HP EliteDesk 705 G3 Small Form Factor PC
- HP EliteDesk 800 G1 Desktop Mini PC
- HP EliteDesk 800 G2 Desktop Mini PC
- HP EliteDesk 800 G1 Small Form Factor PC
- HP EliteDesk 800 G2 Small Form Factor PC
- HP EliteDesk 800 G3 Desktop Mini PC
- HP EliteDesk 800 G3 Small Form Factor PC
- HP EliteDesk 800 G1 Ultra-slim PC
- HP EliteDesk 800/880 G1 Tower PC
- HP EliteDesk 800/880 G2 Tower PC
- HP EliteDesk 800/880 G3 Tower PC
- HP EliteOne 1000 G1 23.8-in All-in-One PC

- HP EliteOne 1000 G1 23.8-in Touch All-in-One PC
- HP EliteOne 1000 G1 27-in Touch 4K UHD All-in-One PC
- HP EliteOne 705 G1 21-inch Non-Touch All-in-One PC
- HP EliteOne 705 G2 23-inch Touch All-in-One PC
- HP EliteOne 800 G1 21.5-inch Non-Touch All-in-One PC
- HP EliteOne 800 All-in-One PC
- HP EliteOne 800 G2 23-inch Non-Touch All-in-One PC
- HP EliteOne 800 G2 23-inch Touch All-in-One PC
- HP EliteOne 800 G3 23.8-inch Non-Touch All-in-One PC
- HP EliteOne 800 G3 23.8-inch Touch All-in-One PC
- HP ElitePOS G1 Retail System Model 141
- HP ElitePOS G1 Retail System Model 143
- HP ElitePOS G1 Retail System Model 145
- HP MP9 G2 Retail System
- HP MP9 G2 Retail System Model 9000
- HP ProDesk 400 G1 Desktop Mini PC
- HP ProDesk 400 G2 Desktop Mini PC
- HP ProDesk 400 G3 Desktop Mini PC
- HP ProDesk 400 G3 Small Form Factor PC
- HP ProDesk 400 G4 Small Form Factor PC
- HP ProDesk 400/480 G1 Small Form Factor PC
- HP ProDesk 400/480 G2 Microtower PC
- HP ProDesk 400/480 G3 Microtower PC
- HP ProDesk 400/480 G4 Microtower PC
- HP ProDesk 400/490/498 G1 Microtower PC
- HP ProDesk 405 G2 Microtower PC
- HP ProDesk 485 G2 Microtower PC
- HP ProDesk 490/498 G2 Microtower PC
- HP ProDesk 490/498 G3 Microtower PC
- HP ProDesk 600 G1 Desktop Mini PC
- HP ProDesk 600 G2 Desktop Mini PC
- HP ProDesk 600 G1 Small Form Factor PC
- HP ProDesk 600 G2 Small Form Factor PC
- HP ProDesk 600 G3 Desktop Mini PC
- HP ProDesk 600 G3 Small Form Factor PC
- HP ProDesk 600/680 G1 Tower PC
- HP ProDesk 600/680 G2 Microtower PC

- HP ProDesk 600/680 G3 Microtower PC
- HP ProOne 400 G1 19.5-inch Non-Touch All-in-One PC
- HP ProOne 400 G1 21.5-inch Touch All-in-One
- HP ProOne 400 G1 23-inch Non-Touch All-in-One
- HP ProOne 400 G2 20-inch Touch All-in-One PC
- HP ProOne 400 G3 All-in-One PC
- HP ProOne 400/460/480 G2 20-inch Non-Touch All-in-One PC
- HP ProOne 600 G1 All-in-One PC
- HP ProOne 600 G2 21.5-inch Non-Touch All-in-One PC
- HP ProOne 600 G2 21.5-inch Touch All-in-One PC
- HP ProOne 600 G3 All-in-One PC
- HP RP5 Retail System Model 5810
- HP RP9 G1 AiO Retail System Model 9015
- HP RP9 G1 AiO Retail System Model 9018
- HP t530 Thin Client
- HP t530 Thin Client
- HP t620 Flexible Thin Client
- HP t620 PLUS Flexible Thin Client
- HP t630 Thin Client
- HP t630 Thin Client
- HP t730 Thin Client
- HP t730 Thin Client
- HP t820 Flexible Thin Client
- HP Z VR Backpack G1
- HP Z
- HP Z1 G3 Workstation
- HP Z2 Mini G3 Workstation
- HP Z238 Microtower Workstation
- HP Z240 SFF Workstation
- HP Z240 Tower Workstation
- HP Z4 G4 Workstation
- HP Z440 Workstation
- HP Z6 G4 Workstation
- HP Z640 Workstation
- HP Z8 G4 Workstation
- HP Z840 Workstation
- HP Z230 MT Workstation

- HP Z230 SFF Workstation
- HP Z228 Microtower Workstation
- TPM 2.0 ver. 7.62.3126.0
- TPM 2.0 ver. 7.62.3126.0
- TPM 2.0 ver. 7.62.3126.0
- TPM 1.2 ver. 6.43.243.0
- TPM 2.0 ver. 7.62.3126.0
- TPM 1.2 ver. 6.43.243.0
- TPM 2.0 ver. 7.62.3126.0
- TPM 1.2 ver. 6.43.243.0
- TPM 2.0 ver. 7.62.3126.0
- TPM 1.2 ver. 4.43 (SLB9660)
- TPM 2.0 ver. 5.62 (SLB9665)
- TPM 2.0 ver. 7.62.3126.0
- TPM 1.2 ver. 4.43.257.0 (SLB9660)
- TPM 2.0 ver. 5.62.3126.0 (SLB9665)
- TPM 2.0 ver. 7.62.3126.0
- TPM 1.2 ver. 4.43.257.0 (SLB9660)
- TPM 2.0 ver. 5.62.3126.0 (SLB9665)
- TBA
- HP ENVY Notebook PC (models 13-ab000 ~ 13-ab099)
- HP Spectre 13 Laptop PC (models 13-af0xx)
- HP Spectre Notebook PC (models 13-v000 ~ 13-v099)
- HP Spectre Notebook PC (models 13-v100 ~ 13-v199)
- HP Spectre x2 12 Detachable PC (models 12-c000~12c-c099)
- HP Spectre x2 Detachable PC (models 12-a000 ~ a099)
- HP Spectre x360 13 Convertible PC (models 13-ae0xx)
- HP Spectre x360 Convertible PC (models 13-4100 ~ 4199)
- HP Spectre x360 Convertible PC (models 13-4100 ~ 4199)
- HP Spectre x360 Convertible PC (models 13-4200 ~ 4299)
- HP Spectrex360 Convertible PC (models 13-w000 ~ 13-w099)
- HP Spectrex360 Convertible PC (models 15-ap000-15ap099)
- HP Spectrex360 Convertible PC (models 15-bl000 ~ 15-bl099)
- HP Spectrex360 Convertible PC (models 15-bl100 ~ 15-bl199)
- OMEN X by HP 17 Laptop PC (models 17-ap000 ~ 17-ap099)
- OMEN X by HP Desktop PC

- HPE Trusted Platform Module 2.0 Kit FW 5.51 - TPM 2.0 FW 5.62 is not affected. This is the Gen9 TPM 2.0 option (only Gen9 servers could have this option). The TPM 2.0 Option for Gen9 servers is not standard on Gen9 servers - it is an option.
- HP ProLiant BL460c Gen9 Server Blade n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HP ProLiant BL660c Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HP ProLiant DL120 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HP ProLiant DL160 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HP ProLiant DL360 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HP ProLiant DL380 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HP ProLiant DL388 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HP ProLiant DL580 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HP ProLiant DL60 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HP ProLiant DL80 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HP ProLiant ML110 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HP ProLiant ML150 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE Apollo 4200 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant DL180 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant DL180 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant DL20 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant DL560 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.

- HPE ProLiant ML10 Gen9 E3-1225 v5 3.3GHz 4-core 8GB-R 1TB Non-hot Plug 4LFF SATA 300W AP Svr/Promo n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant ML10 Gen9 E3-1225 v5 4GB-R 1TB Non-hot Plug 4LFF SATA 300W Svr/S-Buy n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant ML10 Gen9 E3-1225 v5 8GB-R 1TB Non-hot Plug 4LFF SATA 300W Perf Svr n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant ML10 Gen9 E3-1225 v5 8GB-R 2TB Non-hot Plug 4LFF SATA 300W Svr/GO n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant ML10 Gen9 E3-1225 v5 8GB-R 2TB Non-hot Plug 4LFF SATA 300W Svr/TV n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant ML10 Gen9 G4400 4GB-R Non-hot Plug 4LFF SATA 300W Entry Svr n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant ML30 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant ML350 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant ML350 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant XL170r Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant XL190r Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant XL230a Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant XL230a Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant XL250a Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant XL250a Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant XL260a Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.

- HPE ProLiant XL450 Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant XL730f Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant XL730f Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant XL740f Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant XL740f Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant XL750f Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.
- HPE ProLiant XL750f Gen9 Server n/a - only if "HPE Trusted Platform Module 2.0 Kit" w/ FW version 5.51 is installed.

شرکت Lenovo

- Lenovo 100S Chromebook
- Lenovo Flex 11 Chromebook
- Lenovo N20 Chromebook
- Lenovo N21 Chromebook
- Lenovo N22 (Touch) Chromebook
- Lenovo N23 Chromebook
- Lenovo N23 Chromebook (Touch)
- Lenovo N23 Yoga Chromebook
- Lenovo N42 (Touch) Chromebook
- ThinkCentre Chromebox
- ThinkPad 11e Chromebook
- ThinkPad 11e Chromebook 3rd Gen (Yoga/Clamshell)
- ThinkPad 13 Chromebook
- ThinkCentre M710 t/s
- ThinkCentre M710q
- ThinkCentre M715 t/s
- ThinkCentre M910 t/s/q/x
- ThinkPad 13e
- ThinkPad 25
- ThinkPad E460/E560
- ThinkPad E465/E565

- ThinkPad E470/E570
- ThinkPad E475/E575
- ThinkPad L460
- ThinkPad L470
- ThinkPad L560
- ThinkPad L570
- ThinkPad P40
- ThinkPad P50
- ThinkPad P50s
- ThinkPad P51
- ThinkPad P70
- ThinkPad P71 (20Hx)
- ThinkPad T460
- ThinkPad T460p
- ThinkPad T460s
- ThinkPad T470 (20Hx)
- hinkPad T470p
- ThinkPad T470s (20Hx)
- ThinkPad T560
- ThinkPad T570 (20Hx)
- ThinkPad X1 Carbon (20Hx)
- ThinkPad X1 Carbon, X1 Yoga
- ThinkPad X1 Tablet (20Gx)
- ThinkPad X1 Tablet (20Jx)
- ThinkPad X1 Yoga (20Jx)
- ThinkPad X260
- ThinkPad X270
- ThinkPad Yoda 370 /ThinkPad S1 3rd
- ThinkPad Yoga 14 460 S3
- ThinkPad Yoga 260, S1
- ThinkStation P320 Tiny
- ThinkStation P410
- ThinkStation P500
- ThinkStation P510
- ThinkStation P700
- ThinkStation P710
- ThinkStation P900

- ThinkStation P910

شرکت مایکروسافت

- Windows 10 for 32-bit Systems
- Windows 10 for x64-based Systems
- Windows 10 Version 1511 for 32-bit Systems
- Windows 10 Version 1511 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1703 for 32-bit Systems
- Windows 10 Version 1703 for x64-based Systems
- Windows 8.1 for 32-bit systems
- Windows 8.1 for x64-based systems
- Windows RT 8.1
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016