Register | Log in

MAIN MENU MY STORIES: 25 FORUMS SUBSCRIBE JOBS

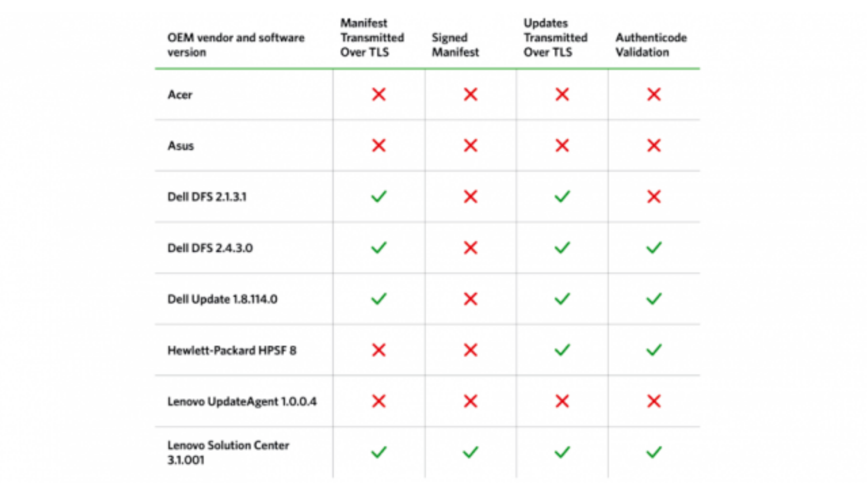
RISK ASSESSMENT / SECURITY & HACKTIVISM

Out-of-the-box exploitation possible on PCs from top 5 OEMs

New study finds third-party updaters are riddled with critical vulnerabilities.

by **Dan Goodin** - Jun 1, 2016 8:26am PDT

120



OEM vendor and software version	Manifest Transmitted Over TLS	Signed Manifest	Updates Transmitted Over TLS	Authenticode Validation
Acer	✗	✗	✗	✗
Asus	✗	✗	✗	✗
Dell DFS 2.1.3.1	✓	✗	✓	✗
Dell DFS 2.4.3.0	✓	✗	✓	✓
Dell Update 1.8.114.0	✓	✗	✓	✓
Hewlett-Packard HPSF 8	✗	✗	✓	✓
Lenovo UpdateAgent 1.0.0.4	✗	✗	✗	✗
Lenovo Solution Center 3.1.001	✓	✓	✓	✓

Duo Security

The next time you're in the market for a new Windows computer, consider this: if it comes from one of the top five manufacturers, it's vulnerable to man-in-the-middle attacks that allow hackers to install malware.

That's the take-away from a report published Tuesday by researchers from two-factor authentication service Duo Security. It found third-party updating tools installed by default threatened customers of Dell, HP, Lenovo, Acer, and Asus. The updaters frequently expose their programming interfaces, making them easy to reverse engineer. Even worse, the updaters frequently fail to use transport layer security encryption properly, if at all. As a result, PCs from all five makers are vulnerable to exploits that allow attackers to install malware.

"Hacking in practice means taking the path of least resistance, and OEM software is often a weak link in the chain," the Duo Security report stated. "All of the sexy exploit mitigations, desktop firewalls, and safe browsing enhancements can't protect you when an OEM vendor cripples them with pre-installed software."

FURTHER READING

DELL DOES A SUPERFISH, SHIPS PCS WITH EASILY CLONEABLE ROOT CERTIFICATES

Root certificate debacle that hit Lenovo now visits the House of Dell.

In short, every single manufacturer was found to use pre-installed updaters that allowed someone with the ability to monitor a PC's network traffic—say someone on the same unsecured Wi-Fi network or a rogue employee at an ISP or VPN provider—to execute code of their choice that runs with System-level privileges. The updaters are mostly used to deliver new versions of software and bloatware that come pre-installed on new PCs and are separate from Microsoft's Windows Update, which is widely believed to be secure. The report provides a strong reason why it's a good idea to wipe newly purchased machines and reinstall Windows minus all the custom crapware. At a minimum, third-party software should be uninstalled or blocked using a firewall.

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

Nvidia GTX 1070 review: Faster than the Titan, at a more reasonable price

Not quite the bargain the 970 was, but the GTX 1070 remains the card to beat.

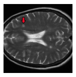
WATCH ARS VIDEO

Sunspring | A Sci-Fi Short Film Starring Thomas Middleditch

For *Sunspring*'s exclusive debut on Ars, we talked to the filmmakers about collaborating with an AI.

STAY IN THE KNOW WITH

LATEST NEWS



Risky stem cell treatment reverses MS in 70% of patients in small study

Prenda lawyers lose key appeal, will pay $230k sanction

BEEP BEEP, WHO'S GOT THE KEYS TO MY SKYJEEP?

Can Google's Larry Page make flying cars a reality?

Update: Lenovo has issued an advisory recommending customers uninstall the Lenovo Accelerator Application, which comes preinstalled on many notebooks and desktop systems running Windows 10. As the image at the top of this post illustrates, the Duo Security report uncovered several major shortcomings in the app's update mechanism, including its failure to use any sort of encryption when checking for or downloading updates and the failure to validate digital signatures before installing them.

READER COMMENTS 120

Dan Goodin / Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.
@dangoodin001 on Twitter

← OLDER STORY NEWER STORY →

YOU MAY ALSO LIKE

LINKEDIN RECS: JUNGLING, TOP LANING
League of Legends admits to using chat-log analysis in employee reviews

Tesla denies suspension issue and accuses blogger of lying

FRIDAY DEALS
Dealmaster: Get a Dell Inspiron 15 7559 for $749.99

SITE LINKS
About Us
Advertise with us
Contact Us
Reprints

SUBSCRIPTIONS
Subscribe to Ars

MORE READING
RSS Feeds
Newsletters

Visit Ars Technica UK

CONDE NAST SITES
Reddit
Wired
Vanity Fair
Style
Details

Visit our sister sites
Subscribe to a magazine

VIEW MOBILE SITE