{* SOFTWARE *}

MS throttles research to conceal SW bugs

The truth will *not* set you free

Thomas C Greene Fri 9 Nov 2001 // 09:21 UTC

EXCLUSIVE Microsoft Security Manager Scott Culp revealed unilateral steps the company has taken to throttle the exchange of vulnerability information relevant to their famously buggy products, clearly in hopes that patches and fixes can be fed to consumers discreetly, without ever realizing they've been at risk to attack.

During a presentation at the Trusted Computing Forum in Mountain View, California Thursday, Culp outlined the terms of several partnerships MS has pursued with compliant security vendors aimed at keeping the Redmond Beast's dirty laundry hidden from the public eye.

Briefly, the scheme requires vendors to withhold detailed security data and to suppress the exchange of exploit code, which, unfortunately, is the only means of verifying that a patch actually works.

Vendors will exercise "best efforts" to avoid disclosing details that can be used to exploit a vulnerability for a period of thirty days from the initial discovery.

After this grace period, or if the Blackhat community begins exploiting it sooner, "additional details" may be released. These details will of course not be sufficient to exploit the flaw, or to test the patch. We would expect the current Microsoft TechNet security bulletins to provide the model of what MS considers to be 'detailed information'.

There will be exceptions for the Feds, for recognized infrastructure protection organizations (ISACS), and "other communities in which enforceable frameworks exist to deter onward uncontrolled distribution."

Clearly, whenever there's fresh trouble, MS is hoping to get the matter resolved quietly and distribute the patches without alarming the public, or drawing attention to its appalling record of security engineering. Win-XP's aggressive auto-update feature will be the prime vehicle of behind-your-back patching, and the .NET initiative will be the needy beneficiary of the false sense of security which the company's new obscurity program will encourage.

Who's Who

The group of security vendors currently collaborating with MS includes some famous, and even ironic, names: @Stake, BindView, ISS, Foundstone, and Guardent. @Stake's Chris Wysopal ('Weld Pond'), an old L0pht denizen, will lead efforts to draft the framework for the new regime. We're much impressed to see how far the L0pht has, em, evolved.

The framework will involve "Members," defined as "Industry-leading companies actively engaged in security research and network defense, and leading software vendors."

Below them will be "Associate Members," defined as "Influential vendors and organizations within the security community who support the goals of the organization."

Finally, we'll have an "Advisory Board," defined as "Influential customers of the security community who support the goals of the organization."

What's wrong with this picture?
While it sounds like a common-sense proposal for limiting damage by restricting access to exploits, the effect of this scheme is likely to be an ironic reduction in security.

For one thing, lines are already being drawn within the security community. There are a number of highly-respected vendors who believe in full disclosure, and who regard Microsoft's partnership arrangement, in which they obviously won't be able to participate, as an assault on the way they do business. Effort will be wasted in fruitless conflict. Information will not be shared, and many talented people will be unable to contribute to the solution because they've not been approved by MS.

The debate over full disclosure is endless and insoluble. Opponents will never agree because there are, quite simply, excellent arguments to which responsible, intelligent, decent people on both sides of the divide adhere.

The two camps have coexisted uneasily, but tolerably, for decades. Now, on the rebound from its gross humiliations by Sircam, Code Red and Nimda, Microsoft has decided it can no longer coexist with the full disclosure camp. But they themselves are to blame for not doing adequate security engineering before releasing their products. They're blaming the messenger because the news so often reflects badly on themselves.

Add to this the fact that exploit code is the only tool for verifying that a workaround or a patch works as it should. Obstructing its dissemination means that non-approved security vendors will have a more difficult time testing their solutions.

When someone devises a security workaround, the first thing they do is attack their machine to see if it works. Ideally, one attacks it using as many exploits as one can find. If you have a vendor handling this for you, then its in your best interest to see that they've tested their solution as rigorously as possible. This requires an exchange of information. A apartheid system of 'approved' and 'rogue' security vendors is hardly beneficial to consumers of these services.

Because MS has moved in secret, making back room deals with a select few, it's possible that opponents of this scheme will be tempted to retaliate by aggressively searching for exploitable holes in MS products and publicizing the information widely, in order to demonstrate the futility of security through obscurity. Any such 'disclosure war' would only make end users less secure.

But the best and most dramatic example of the folly of obscurity is the recent fiasco with MS Passport session cookies, first reported by security researcher Marc Slemko. Millions of Passport users were open to an attack which could have revealed extremely sensitive personal and financial data.

In this case, Slemko did the right thing by publishing the exploit. Microsoft immediately disabled Passport services until a workaround could be implemented.

However, had MS handled it according to their new disclosure regime, all of

those customers would have remained open to attack for up to a month, entirely innocent of the danger.

This works for Microsoft, which wants you to trust its many .NET services whether you ought to or not. It doesn't work for end users. MS would have tossed the dice hoping that the flaw wouldn't have been exploited before they got it fixed. But the extremely sensitive nature of the information at risk in this case means that even a fairly safe bet is a bad idea.

By publishing the exploit Slemko ensured that MS would move immediately; and furthermore, he demonstrated the relative ease with which a session can be hijacked. Now users of these services will be a good deal more cautious about the sort of information they'll trust to Microsoft. Surely, we're all better off knowing that Passport is essentially insecure.

Your Mum was right; honesty really is the best policy. ®

Related Stories

MS to force IT-security censorship
MS Passport cracked with Hotmail

Leaked: List of police, govt, uni orgs in Clearview AI's facial-recognition trials

Plus: Mortgage algorithm bias, and an AI-guided play comes to London

Katyanna Quach Sun 29 Aug 2021 // 09:48 UTC 2

IN BRIEF Clearview AI's controversial facial-recognition system has been trialed, at least, by police, government agencies, and universities around the world, according to newly leaked files.

Internal documents revealed by BuzzFeed News show that Clearview offered its technology to law enforcement agencies, governments, and academic institutions in 24 countries, including the UK, Brazil, and Saudi Arabia, on a try-before-you-buy basis.

The facial-recognition biz scraped billions of photos from public social media profiles, including Instagram and Facebook, and put them all into a massive database. Clearview's customers can submit pictures of people and the system will automatically try to locate those people in the database, using facial recognition, and return any details picked up from

their personal pages if successful. Thus, the police can, for example, give

CONTINUE READING

Real world not giving you enough anxiety? Try being hunted down by the perfect organism in *Alien: Isolation*

2014 stealth-em-up hasn't aged a day

Richard Currie Sat 28 Aug 2021 // 10:37 UTC **11**

THE RPG *Greetings, traveller, and welcome back to* The Register Plays Games*, our monthly gaming column. Not that anybody noticed but we skipped the last edition for a number of reasons.* ***1)*** *Too many betas. Though we were monitoring developments in potential* World of Warcraft *killer* New World *and* Left 4 Dead's *spiritual successor,* Back 4 Blood*, we didn't see anything that could be discussed fairly.* ***2)*** *Generally no new full releases of interest.* ***3)*** *We had to RMA a graphics card and got sad. However, when setting out the vision for this column, there were no hard and fast rules about what got covered. So this time we're headed back to 2014 and a crumbling space station where something extremely violent and dangerous lurks in the shadows…*

I own two copies of *Alien: Isolation*. The first was bought on disc for the Xbox One at release seven years ago. At this point I had never truly committed to a "survival horror" simply because, while horror films and literature are great, horror games are another kettle of fish.

The flicking of pages and glow from the big screen are gentle reminders

CONTINUE READING

Et tu, Samsung? Electronics giant accused of quietly switching SSD components

Squirrely semiconductor swaps make performance difficult to predict

Thomas Claburn in San Francisco Sat 28 Aug 2021 // 08:08 UTC **42**

Samsung has altered the parts used to make its 970 EVO Plus 1TB SSD card, leading a version manufactured in June 2021 to perform differently than an older formulation from April 2021.

In a video posted to the channel YouTube channel 潮 玩 客 ("Trendy Player"), Chinese video blogger Jian Ge recently compared two versions of the product – one from April labelled with part number MZVLB1T0HBLR and another from June labelled MZVL21T0HBLU – and found the performance characteristics have changed, some for the better and some for the worse.

CONTINUE READING

Microsoft warns of widespread open redirection phishing attack – which Defender can block, coincidentally

Some tactics never change much

Thomas Claburn in San Francisco Fri 27 Aug 2021 // 21:59 UTC 7

Microsoft has warned that it has been tracking a widespread credential-phishing campaign that relies on open redirector links, while simultaneously suggesting it can defend against such schemes.

"Attackers combine these links with social engineering baits that impersonate well-known productivity tools and services to lure users into clicking," the company's Microsoft 365 Defender Threat Intelligence Team said in a blog post on Thursday.

"Doing so leads to a series of redirections – including a CAPTCHA

CONTINUE READING

Perseverance to take a second stab at Martian rocks ... but first it has to scratch'n'sniff

Hopefully this'll be the sample that eventually gets sent back to Earth

Katyanna Quach Fri 27 Aug 2021 // 20:56 UTC 6

NASA's Perseverance rover will make a second attempt at collecting a sample of Mars rock for eventual return to Earth – though it's going to scratch its latest target first to make sure it's worth bothering.

The 1,025-kg, nuclear-powered trundlebot may be the most advanced vehicle to explore Mars yet, but it proved no match for some parts of the Red Planet's regolith. On its first sampling attempt, it bored a hole into a patch of ground in the Jezero crater, but no material was bottled up, leaving the boffins baffled.

An analysis showed that the machine's software and hardware was operating flawlessly. There was nothing wrong with Perseverance, it's

CONTINUE READING

Microsoft does and doesn't want you to know it won't stop you manually installing Windows 11 on older PCs

Hardware requirements loophole left in

Chris Williams, Editor in Chief Fri 27 Aug 2021 // 20:25 UTC 52

Microsoft doesn't want to say it publicly but it will not stop you manually installing Windows 11 on older or otherwise incompatible PCs.

The Redmond giant is under fire for the stringent hardware requirements of its upcoming operating system, due to be formally released by the end of the year.

To be officially supported by Windows 11, machines will need TPM 2.0 support; an eighth-generation or newer Intel Core processor, a Zen 2 or

CONTINUE READING

Dell, HP talk of backlogs and shortages as big PC-makers turn in their numbers

Dell's results were upbeat, HP's flat, but investors still worried over supply chain

Jude Karabus Fri 27 Aug 2021 // 19:05 UTC **2**

HP Inc and Dell both raised concerns over ongoing component shortages when they reported their July quarters yesterday, with the Palo Alto firm citing "unprecedented demand that is way ahead of supply right now" and Round Rock saying "demand was ahead of revenue growth as we managed supply constraints."

Dell's PC biz saw growth in its enterprise rather than consumer segment for its fiscal Q2, with revenue from its client-solutions group, which mainly sells PCs, up 27 per cent to $14.3bn.

HP's PC results, by contrast, were flat, with its Personal Systems unit

CONTINUE READING

'Apps for GNOME' site aims to improve discovery of the project's best applications

A sprinkling of Rust and presto! A new multi-language web site appears

Tim Anderson Fri 27 Aug 2021 // 18:05 UTC **4**

The GNOME project has created Apps for GNOME, a website to "feature the best applications in the GNOME ecosystem," according to creator Sophie Herold.

The scope of the GNOME project is extensive and includes low-level system components, a toolkit for developers of GUI applications (GTK), a desktop shell and window manager, and numerous applications built with these technologies.

GNOME apps fall into three categories. The first, called Core, are apps

CONTINUE READING

EU to formally probe Nvidia's $54bn takeover over British chip designer Arm – report

Hot on heels of 'significant concerns' from the UK

Gareth Corfield Fri 27 Aug 2021 // 16:58 UTC **20**

Nvidia told *The Reg* it would work "with the European Commission to address any concerns they may have" after reports it is set open a formal competition law investigation into the AI firm's purchase of Arm from Softbank.

The *Financial Times* reported this morning that the political bloc will examine whether or not the $54bn takeover deal will result in reduced competition between the world's leading chip designers.

"The investigation is likely to begin after Nvidia officially notifies the European Commission of its plan to acquire Arm," said the UK financial

CONTINUE READING

Slap on wrist for NCC Group over CREST exam-cheating scandal as infosec org agrees to rewrite NDAs and more

Two 'historic' incidents nearly a decade ago, says statement

Gareth Corfield Fri 27 Aug 2021 // 15:55 UTC 4

British infosec firm NCC Group has been rapped over the knuckles after infosec accreditation body CREST found it was "vicariously responsible" for employees who helped staff cheat certification exams.

In a lengthy statement published yesterday, CREST said last summer's exam-cheating scandal boiled down to just two incidents carried out between the years 2012 and 2014.

"On two occasions between 2012 and 2014, the examination-related activities of one of more NCC Group employees and candidates

CONTINUE READING

This way up: James Webb Space Telescope gets ready for shipment after final tests

Next stop, Kourou

Richard Speed Fri 27 Aug 2021 // 14:30 UTC 21

It's been a big week for the much-delayed James Webb Space Telescope (JWST) as testing of the observatory was completed and operations to ship the spacecraft to the Kourou launchpad began.

It has been a long time coming – the best part of 25 years since development started – but it looks very much the JWST will finally head to space this year.

A poster child for cost overruns, the JWST is a joint NASA, ESA and CSA project and will make observations in a lower frequency range than the

CONTINUE READING