MicroSolved, Inc. Presents:

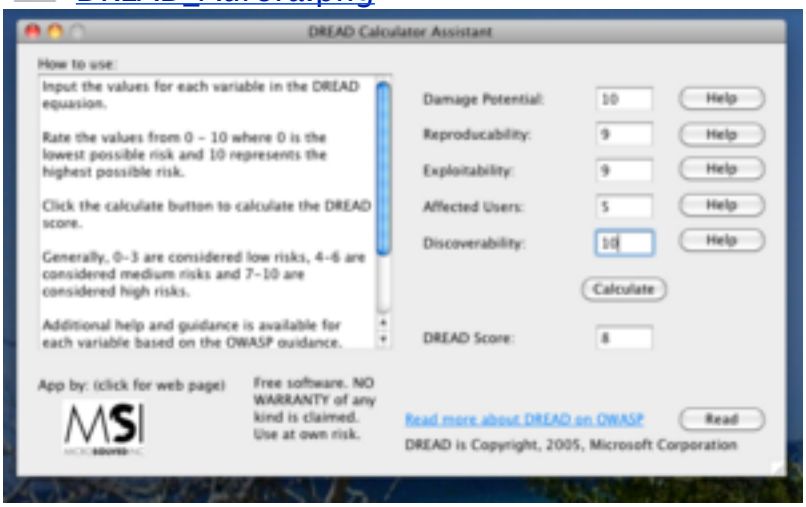
FLASH Campfire Chat: The Aurora Vulnerability

January 22, 2010

9:45 AM

Brent H.

DREAD_Aurora.png



10:00 AM

Brent H.	First of all, thanks for coming.
	Your time is very valuable, so I appreciate you joining us.
Brent H.	We are here to discuss the so called "Aurora vulnerability"
	Mcafee called it Operation Aurora and the name stuck. http://hurl.ws/aj6c
	MS calls it: MS10-002 and the advisory is here: http://hurl.ws/afjs and deeper here: http://hurl.ws/afjt
	Hopefully, that is the topic that folks were attending to discuss. :)

pophop	Summary?
Brent H.	I am going to ignore the hype around who got compromised and all of that and focus, instead on the vulnerability, suggested controls for risk minimization and those details.
	The summary is that there exists a vulnerability in Internet Explorer that allows a malicious content to execute remote code in the context of the user viewing the content.
	Affected versions: Internet explorer 5.01 – 8 prior to the patch installation
	The vulnerability allows remote code execution. The execution is contextual, so code runs as the user.

10:10 AM

Brent H.	Basically, like many of the things we have seen before, these vulnerabilities can be used to establish a beachhead on your environment and install malicious code.
pophop	Attack scenario?
Brent H.	This gives attackers a gateway to escalate privs, perform pivot attacks and other mechanisms.
Brent H.	There is a great video of the Metasploit exploit here: http://hurl.ws/ajwy
	There are several versions of the exploit in the wild. Some have basic shells, some have download trojan executions. Many have overcome DEP and other protections.
	The attack vector does require getting your victim to visit the malicious site. This can be done by social engineering, XSS, CSRF, etc. There are a thousand ways.
	In the past we have seen everything from emails to web infections, from sms spam to physical flyers, etc. People will visit bad sites. You can't block everything.
pophop	Similar vilns have appeared in IE before – why is this one any different?

Brent H.	So, pophop, the vector is to get a person to follow a link or view malicious content on the web.
	IMHO, it is not different, other than the fact that it extends across such a wide range of versions.
pophop	ahh... so no "go to IE8 " solution...
Brent H.	The only other thing unique about this is that so many variants of the exploit exist and have existed before the patch.
pophop	got it
Brent H.	Once the metasploit exploit was available, we saw a storm of different exploit code emerge, very quickly.
	IE8 was initially claimed to be vulnerable but not exploitable.
pophop	how to detetct in network logs? any way?
Brent H.	However, emerging exploits proved that DEP could be bypassed and that exploitation IS POSSIBLE.
	Nessus has a signature to detect the missing patch: http://hurl.ws/ag7s

10:15 AM

Brent H.	MSI Guarddog clients will be assessed during your next scheduled assessment for this patch. If you need faster checking, simply request a focused assessment for this particular vuln.
	AV detection varies by product and exploit. Many of the exploits we checked were widely missed by lower-end anti-virus. As always, polymorphism should be expected, which m,ay defeat much of the AV infrastructure.
	Signatures for some of the exploits are available on various NIDS platforms at this point as well as in some of the web-filtering and DLP solutions/proxies.
	Because this is a client-side exploit and many folks never look at the logs or integrity of their workstations, detection is difficult using normal mechanisms

You also have to consider that the exploits have been known for some time before the patch, so it may already have been leveraged to gain a beachhead in your environment

I want to segue for a second and discuss the risk rating for this vuln and exploit.

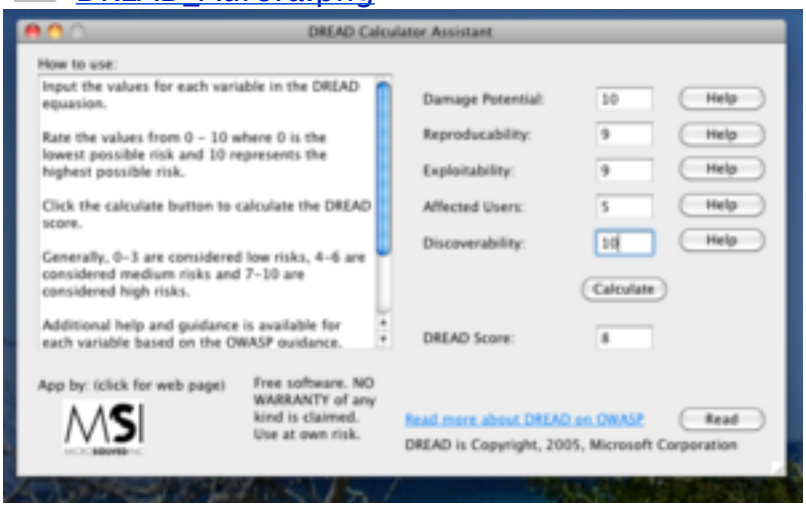
To the right of your screen, you should see a downloadable link to a file called DREAD_Aurora.png

This is a DREAD metric model that we did for this threat condition. Our analysis rates this vulnerability as an 8 out of 10 (HIGH). You can see the scores in the graphic.

10:20 AM

Brent H.

DREAD_Aurora.png



The tool used to perform this analysis is available for FREE from microsolved.com in our free tools area.

Sorry for that, you have to be in the room when it is uploaded. :)

I mention this risk rating purely to help folks decide about what their responses will be.

Many folks said that they had pushed the patch already to a number of workstations. Have those that have pushed the patch had any issues or problems?

Kenneth J.	Have not heard of any issues.
Brent H.	BTW - here is the link to the DREAD tool: http://hurl.ws/aj6j
Rod C.	none heard of
pophop	Daltech: all OK with patch?
Brent H.	Our research did not show anyone having any issues with the patch either.
Todd F.	Following install yesterday, IE 8 couldn't find the proxy, but was corrected by restarting IE
Brent H.	Our test machines experienced no problems and we have not heard of stability issues.
	So, basically, don't wait for stability or anything to push the patch.

10:25 AM

Brent H.	So far, other than Todd's issue, we have heard no negatives about it.
	I also want to comment on a couple of longer term ideas.
	n terms of defenses, the best approach seems to be to deploy defense in depth.

	View paste
	`This is an excellent example of where orgs that have embraced the 80/20 rule, particularly enclaving and egress components, are feeling little pressure from this vulnerability.`
	`They have accounted for this, and the potentially thousands, of other 0-day client-side attacks on the horizon.`

	The feedback we have heard from those with strong egress filtering and enclaving in place, is that they were not spending much attention on this vulnerability specifically.,,
pophop	desktop space security erosion just gets worse...
Brent H.	IN many cases, people have begun to account for initial stage compromises through client-side attacks.

	This is a great example of why architecting your environment for initial levels of security failure are very wise.
Brent H.	How many folks have enclaved or segregated their workstations from other parts of their environments?
Brent H.	This might be a good point to discuss this.... IE really needs to get replaced.

10:30 AM

Robert R.	I'll 2nd that.
pophop	We have enclaved - imperfectly.
Brent H.	A longer term initiative would be to remove IE from day to day use for external content that doesn't require it.
pophop	How to convince management / culture?
Brent H.	You can check out our advice on this here: http://hurl.ws/ag7t - IE replacement
	Sorry for the cut off lines. I will try and keep them shorter, if that helps.
	Management needs to be convinced by making an actuarial risk argument
	You can discuss the costs and risks of IE on the desktop for general Internet use
Nick B.	intranet apps which requrie old IE trump security, apparently.
	and who wants to spend money to upgrade old apps?
	or worse, to hire coders to update home-brew apps?
Brent H.	See our article at the URL, intranet use is probably OK
	But, you have to try and get controls in place to regulate Internet use
pophop	Block IE at proxies - but then laptops go home.
Brent H.	True, they do. These are things you can't manage with a single control.

	You need to establish controls in depth that control IE use of explorer
	Plus implement enclaving and other preventative and detective controls to manage variance
	Basically, if you see something in user land as high risk, you can take steps to limit it
	Then establish additional risk minimization controls and detective controls around the behavior
Kenneth J.	I'm a novice, what is enclaving

10:35 AM

Brent H.	Here is a good write up of this approach: http://securityblog.verizonbusiness.com/20…
	Enclaving is the act of segregating your network into zones of trust
pophop	so desktops do noy have direct access to production space
Brent H.	You create enclaves for workstations, servers by function/risk/line of business, etc.
	Thus you create zones of control that limit the impact of a first stage compromise
	So Kenneth, if I happen to exploit one of your workstations and get a shell back
	the point of enclaving is to use firewalls, ACLS and detective controls to limit what I can do
Robert R.	Brent: Are VLAN's enough to separate the zones or should it require more?
Brent H.	where I can go and what I can access with my stolen capability

	VLANS can be effective if other controls are in place and the core switch is truly secured
pophop	VLAB ACL's ?
	VLAN
Brent H.	They should not be relied upon solely for security or as a single control, but can be part of a defense in depth strategy
Robert R.	True. I should have mentioned ACL's in there also ;) Not just VLAN's alone.
Brent H.	I would be very careful about using VLANs across wide zone of trust disparities though.
	For example, I probably would not use VLANS to segregate a highly sensitive network from an Internet DMZ
	but internally. across similiar models of trust, if the switch fabric is secure, I would consider it

10:40 AM

Brent H.	Of course, with ACLs. They are an additional and low cost control.
	My bottom line point on this is that organizations who understand that this is an example
	but won't be the last 0-day we see for client-side attacks
	and begin to undertake processes like egress, enclaving and other parts of a leveraged security approach
	will be miles ahead when the next black swan is born.
pophop	The fact that desktop space is lost is what people have to accept - and then deal with it. That leads to segregation of core components: enclaving.

Brent H.	They will already have controls to minimize risk of initial stage compromises and will feel less pressure from these types of attacks in the future.
	Absolutely.
	Plus, Internet Explorer is only one example.
	How many folks have 3rd party apps on their workstations?
Robert R.	everybody?
Brent H.	Adobe, VLC, Skype, various freeware tools, WinZIP, etc.
	These are all targets and continue to be popular among the underground.
	Trying to regulate desktop apps is a losing battle. The govt cant even do it in classified environments.
	Thus, we have to engineer for risk minimization with the idea that we can't mitigate these exposures
	That is a core of our 80/20 rule of infosec approach and all of the designs and architecture projects in it

10:45 AM

Brent H.	Enclaving and egress are core focuses, but others have high payoffs too
	So, before I move on to a bit of humor from this security issue, what questions do we have?
pophop	Wait - can we assume desktop content is lost?
Brent H.	You should understand that there may already be compromised hosts in your desktop population

	But, this is true usually anyway.
	Thus you should be doubling your efforts around identifying potentially anomalous behaviors from workstations
	Running routine AV scans of all desktops
	Deploying detective controls in the desktop space to identify bad behavior or scanning
pophop	and endless and losing game it seems.
Brent H.	Basically, you should think of the risk metric as right now, it is probably twice as likely that you may have a compromised desktop in your environment as usual.
	Exactly my point.
	If you have not already begun enclaving, egress and deploying anomaly detective controls you need to do so, use this event as a catalyst
pophop	If we accept that all desktop content is lost and refuse to allow important stuff to even reside on desktops we can abandon desktop space entirely - I think that is inevitable.

10:50 AM

Brent H.	You also have to perform some work to identify potentially already compromised workstations using the tools you have
	I agree that it is inevitable
	Organizations will have to adopt enclaved architectures and allow for initial stage compromises.
	Risk minimization is what is needed.
	also, BTW, if you have not already done so, PUSH THE PATCH. :)
	There is no need, especially in this case, to keep the vuln window open longer than needed.

	This exploit and compromises from it will be living on for a while. There are simply too many consumer victims
	for it to drop off.
	We will also likely see a huge increase in bot-net activity, sql-injection defacements to spread the exploit code and XSS attacks to leverage user trust
	So, secondarily, you should focus on ensuring that you have these areas under control as well.
	To date, much of the focus has been on corporations and corporate users, but consumers, home banking users, etc. will be the second ring targets, if they are not already.
	You can expect more of the joy that client-side malware brings in the next few months, because the target pool is huge!

10:55 AM

pophop	Our logs indicate much of the evil happens at home - on company computers.
Brent H.	Much of it probably does. Much of it probably happens to mobile devices as they move around the world.
	Anyone want to talk about how many cycles they have spent on client-side malware in the last year?
	Things like the Zeus bot and others are making significant improvements in capability and threat levels,
pophop	Ha! - much. Probably 3/4 guys full time integrated over globe.
Brent H.	they are subtle, effective and difficult to detect. Client-side malware is a huge emerging threat.
pophop	Proxy-aware?
Brent H.	I believe we will only see more and more in 2010-2012. You will see more probability and more impact, maybe even exponential growth

	Of course they have become proxy-aware. They are fully capable of avoiding detection in many cases.
	Can anyone here discuss some of their experiences with Zeus?
	Zeus was an extremely powerful malware kit. It was designed to do much of the man-in-the-browser style work without the need for kernel hooks.

11:00 AM

pophop	Doubt if most would even know its presence.
Brent H.	It watched sessions, tampered with session content, changed values, tricked users into logging into fake client-side screens, etc.
	Oh believe me, some folks know a lot about it. It has been very prevalent around financial orgs for the last few months.
	Theft of credentials and money has been high.
	Those are the kinds of threats that these type of client-side exploits will breed.
pophop	How did they become aware?
Robert R.	Wow - haven't even heard of it myself.
Brent H.	Sure, you will see corporate targeting, as we have here with Google, et al, but you will see wide-scale focus on consumer systems who are very slow to patch,
Brent H.	They became aware, not through technical means, but through the identification of the fraud caused by it.
Robert R.	They have me stuck as our content editor and I don't get as much security research time as I used to. I'll have to read up on that more.

Brent H.	As is the case in most events (read the Verizon report), real-world fraud is usually the trigger to investigate the cyber-issues.
pophop	Cuckoo's Egg stuff... billing anomalies... ;-)
Brent H.	It is a good read. Very interesting.
	Yes, direct theft of assets.
	Here is a quick link to an article that describes it and its use of cloud services from Amazon for command and control. http://hurl.ws/ajxa
	You can read a lot more beyond that with an easy Google search.

11:05 AM

Brent H.	OK folks, it has been an hour or so, does anyone have any more questions?
	Reading the Microsoft advisories is very interesting.
	I particularly like this bit of advise from the advisory: "Manage the software and security updates you need to deploy to the servers, desktop, and mobile computers in your organization."
	That seemed like, pretty much, a no-brainer to me.
Mary R.	A reminder for those who joined us after the chat started. We will have a transcript available.
pophop	Thanks - this has been good!
Rod C.	Thanks for the chat
Brent H.	I also got someone who said, just don't use Internet Explorer to open web content....
Robert R.	I have one but it may be slightly off topic.

Brent H.	Thanks all for attending
	Sure. go ahead Robert
Robert R.	We have no patch management in place where I work. Generally, what are my options? Remember I'm normally just a Linux guy.
Brent H.	You can get everyone to run Windows update.
	Are you on a Windows AD infrastructure?
Robert R.	That's what we *try* to do now ;) It doesn't work too well. Yes we have a windows 2003 AD
Brent H.	If so, you could build a login script for everyone to run Windows Update for them when they login next.
	Then, force everyone to logout and lob back in.
Robert R.	Good point. Is there any patch management capabilities in Windows Server 2k8?

11:10 AM

Brent H.	Not sure about built in patch management. But you can certainly use a variety of third party tools to do it. Thinks like LanGuard, etc. have patching capabilities if you are a forest or domain admin.
Brent H.	There are also likely some open source tools and freeware available.
Robert R.	Were looking at trying to upgrade our AD server anyhow and I wanted to look into implementing patch management in the process.
	Alright. Thanks for the great chat event and thanks for your time.
Brent H.	You definitely should do so.
	Thanks all and have a great weekend!

For more information or to join our mailing list so we can let you know of future chat dates, please send your contact information to: Mary Rose Maguire at mmaguire@microsolved.com