

Could a few lines  
of code F@#k it all  
up?

# Dependencies

- Probably 90% of commercial application make use of Open Source Software
- Open Source is great but....
- Node.js is quickly becoming a leading framework for web development
- Some features of node's repository are concerning from the security point of view

# The Left-Pad Saga

## Azer Koçulu

A fairly anonymous developer at that time decided to “Liberate” his modules following a disagreement with NPM staff.

Among them was a module named Left-Pad



Azer Koçulu

Follow

Homepage: <http://azer.bike>

Mar 22, 2016

### I've Just Liberated My Modules

*Note: Thank you for all the support* ❤️

# The Left-pad Saga



**silkentrance** commented on Mar 22

When building projects on travis, or when searching for left-pad on npmjs.com, both will report that the package cannot be found.

Here is an excerpt from the travis build log

```
npm ERR! Linux 3.13.0-40-generic
npm ERR! argv "/home/travis/.nvm/versions/node/v4.2.2/bin/node" "/home/travis/.nvm/versions/node/v4
npm ERR! node v4.2.2
npm ERR! npm v2.14.7
npm ERR! code E404
```

```
npm ERR! 404 Registry returned 404 for GET on https://registry.npmjs.org/left-pad
```

```
npm ERR! 404
npm ERR! 404 'left-pad' is not in the npm registry.
npm ERR! 404 You should bug the author to publish it (or use the name yourself!)
```

```
npm ERR! 404 'left-pad' is not in the npm registry.
```

```
npm ERR! 404 You should bug the author to publish it (or use the name yourself!)
```

```
npm ERR! 404 carbali, folder, http url, or git url.
npm ERR! Please include the following file with any support request:
npm ERR!    /home/travis/build/coldrye-es/pingo/npm-debug.log
make: *** [deps] Error 1
```

# The Left-Pad Saga

- Left-Pad was used by ~40 npm modules – up to 370 now
  - including React and Babel (used by FB, AirBnB and others)
- First of all Azer is no longer anonymous.
- He actually triggered an important discussion within the community:
  - Should an author be able to un-publish his work without a process?
  - What happens to the available module names?



The background of the slide features a solid blue gradient. Scattered across this background are several three-dimensional purple cubes of varying sizes and orientations. Some cubes are in sharp focus, while others are blurred, creating a sense of depth. The cubes are arranged in a non-uniform, architectural pattern.

# The NPM Platform

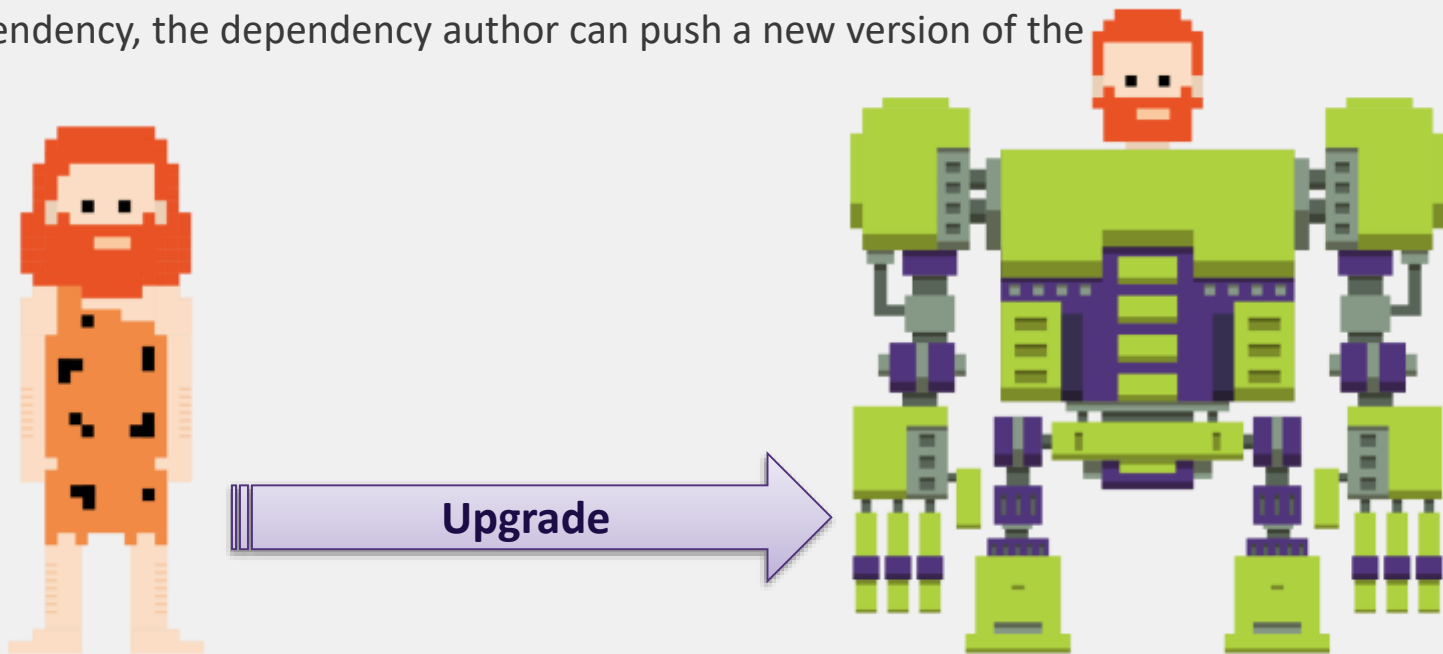
# npm– Node.js Package Manager

- NPM is the node.js open source package manager, command-line client, and a centralized registry of Node.js modules
- “Find, share, and reuse packages of code from hundreds of thousands of developers”
- Over 435,000 modules used by over 6.5 million developers



## Some points to note about npm registry

- Semantic Versioning – npm encourages the use of [semver](#), or semantic versioning.
  - Dependencies are not locked to a certain version by default.
  - For any dependency, the dependency author can push a new version of the package.





## Some points to note about npm utility

- Persistent authentication – npm utilizes persistent authentication to the npm server.
  - Users are not logged out until they manually do so
  - Typing 'npm install' may allow any module to execute arbitrary publish commands

Of course  
I am Superman.



## Some points to note about npm repo

- Centralized registry – NPM utilizes a centralized registry
  - Typing *npm publish* ships your code to this registry server, where it can be installed by anyone.

**“activedirectory”**

## LDAP client for AuthN and AuthZ

## 4 Dependencies?

[illegible]

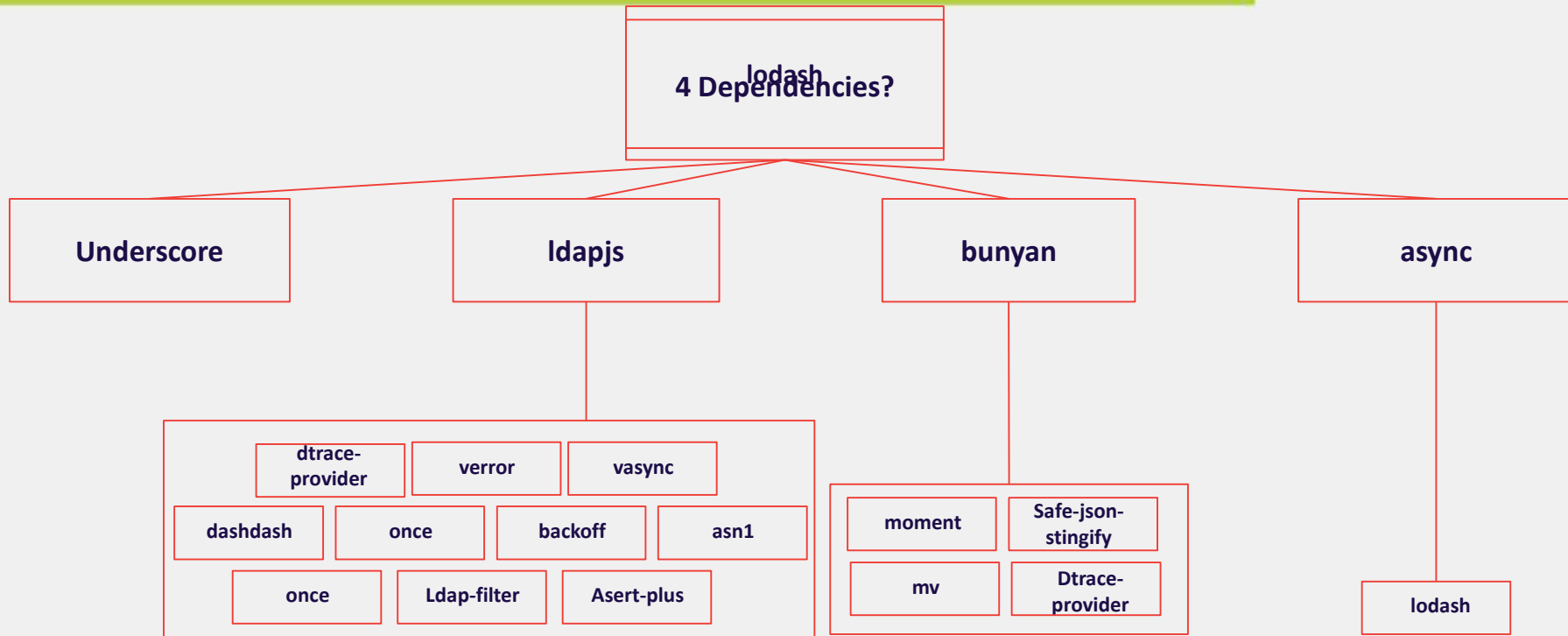
**~3k weekly  
downloads**

## 4 Dependencies?

So simple - `npm install <module name>`

```
C:\data\DB\SQLInjectionMongoDBGet>  
C:\data\DB\SQLInjectionMongoDBGet>
```

# Lets take an example npm



$$4+10+4+1=19$$

# What about lodash?

lodash

~71k Dependents!

42,866,114  
downloads last  
month!

0 Dependencies?

The screenshot displays the official npm page for the 'lodash' package. It includes the package name 'lodash', a description 'Lodash modular utilities.', and a note that it is a fork of the Underscore.js project. The 'Installation' section provides commands for installing via npm or yarn. The 'Usage' section shows how to import and use various lodash functions like '\_.clone', '\_.map', and '\_.filter'. The 'Support' section lists supported environments. On the right, statistics show 42,866,114 downloads last month and 0 dependencies. A list of dependents is also visible at the bottom.

**lodash**  
Lodash modular utilities.  
This is a **fork** of the original Underscore.js project.

**Installation**  
Install npm:  
`$ npm install -g npm`  
`$ npm install -g lodash`

**Usage**  
To clone the first object:  
`var _ = require('lodash');  
var clone = _.clone({ 'a': 1, 'b': 2 });  
clone.a = 10;  
clone.b = 20;  
clone.c = 30;  
clone.d = 40;  
clone.e = 50;  
clone.f = 60;  
clone.g = 70;  
clone.h = 80;  
clone.i = 90;  
clone.j = 100;  
clone.k = 110;  
clone.l = 120;  
clone.m = 130;  
clone.n = 140;  
clone.o = 150;  
clone.p = 160;  
clone.q = 170;  
clone.r = 180;  
clone.s = 190;  
clone.t = 200;  
clone.u = 210;  
clone.v = 220;  
clone.w = 230;  
clone.x = 240;  
clone.y = 250;  
clone.z = 260;  
clone.aa = 270;  
clone.ab = 280;  
clone.ac = 290;  
clone.ad = 300;  
clone.ae = 310;  
clone.af = 320;  
clone.ag = 330;  
clone.ah = 340;  
clone.ai = 350;  
clone.aj = 360;  
clone.ak = 370;  
clone.al = 380;  
clone.am = 390;  
clone.an = 400;  
clone.ao = 410;  
clone.ap = 420;  
clone.aq = 430;  
clone.ar = 440;  
clone.as = 450;  
clone.at = 460;  
clone.au = 470;  
clone.av = 480;  
clone.aw = 490;  
clone.ax = 500;  
clone.ay = 510;  
clone.az = 520;  
clone.ba = 530;  
clone.bb = 540;  
clone.bc = 550;  
clone.bd = 560;  
clone.be = 570;  
clone bf = 580;  
clone.bg = 590;  
clone.bh = 600;  
clone.bi = 610;  
clone.bj = 620;  
clone.bk = 630;  
clone.bl = 640;  
clone bm = 650;  
clone.bn = 660;  
clone.bo = 670;  
clone.bp = 680;  
clone bq = 690;  
clone.br = 700;  
clone.bs = 710;  
clone.bt = 720;  
clone bu = 730;  
clone bv = 740;  
clone bw = 750;  
clone bx = 760;  
clone by = 770;  
clone bz = 780;  
clone.ca = 790;  
clone.cb = 800;  
clone.cc = 810;  
clone.cd = 820;  
clone.ce = 830;  
clone.cf = 840;  
clone.cg = 850;  
clone.ch = 860;  
clone.ci = 870;  
clone.cj = 880;  
clone ck = 890;  
clone.cl = 900;  
clone cm = 910;  
clone.cn = 920;  
clone.co = 930;  
clone.cp = 940;  
clone cq = 950;  
clone cr = 960;  
clone cs = 970;  
clone.ct = 980;  
clone cu = 990;  
clone cv = 1000;  
clone cw = 1010;  
clone cx = 1020;  
clone cy = 1030;  
clone cz = 1040;  
clone da = 1050;  
clone db = 1060;  
clone dc = 1070;  
clone dd = 1080;  
clone de = 1090;  
clone df = 1100;  
clone dg = 1110;  
clone dh = 1120;  
clone di = 1130;  
clone dj = 1140;  
clone dk = 1150;  
clone dl = 1160;  
clone dm = 1170;  
clone dn = 1180;  
clone do = 1190;  
clone dp = 1200;  
clone dq = 1210;  
clone dr = 1220;  
clone ds = 1230;  
clone dt = 1240;  
clone du = 1250;  
clone dv = 1260;  
clone dw = 1270;  
clone dx = 1280;  
clone dy = 1290;  
clone dz = 1300;  
clone ea = 1310;  
clone eb = 1320;  
clone ec = 1330;  
clone ed = 1340;  
clone ee = 1350;  
clone ef = 1360;  
clone eg = 1370;  
clone eh = 1380;  
clone ei = 1390;  
clone ej = 1400;  
clone ek = 1410;  
clone el = 1420;  
clone em = 1430;  
clone en = 1440;  
clone eo = 1450;  
clone ep = 1460;  
clone eq = 1470;  
clone er = 1480;  
clone es = 1490;  
clone et = 1500;  
clone eu = 1510;  
clone ev = 1520;  
clone ew = 1530;  
clone ex = 1540;  
clone ey = 1550;  
clone ez = 1560;  
clone fa = 1570;  
clone fb = 1580;  
clone fc = 1590;  
clone fd = 1600;  
clone fe = 1610;  
clone ff = 1620;  
clone fg = 1630;  
clone fh = 1640;  
clone fi = 1650;  
clone fj = 1660;  
clone fk = 1670;  
clone fl = 1680;  
clone fm = 1690;  
clone fn = 1700;  
clone fo = 1710;  
clone fp = 1720;  
clone fq = 1730;  
clone fr = 1740;  
clone fs = 1750;  
clone ft = 1760;  
clone fu = 1770;  
clone fv = 1780;  
clone fw = 1790;  
clone fx = 1800;  
clone fy = 1810;  
clone fz = 1820;  
clone ga = 1830;  
clone gb = 1840;  
clone gc = 1850;  
clone gd = 1860;  
clone ge = 1870;  
clone gf = 1880;  
clone gg = 1890;  
clone gh = 1900;  
clone gi = 1910;  
clone gj = 1920;  
clone gk = 1930;  
clone gl = 1940;  
clone gm = 1950;  
clone gn = 1960;  
clone go = 1970;  
clone gp = 1980;  
clone gq = 1990;  
clone gr = 2000;  
clone gs = 2010;  
clone gt = 2020;  
clone gu = 2030;  
clone gv = 2040;  
clone gw = 2050;  
clone gx = 2060;  
clone gy = 2070;  
clone gz = 2080;  
clone ha = 2090;  
clone hb = 2100;  
clone hc = 2110;  
clone hd = 2120;  
clone he = 2130;  
clone hf = 2140;  
clone hg = 2150;  
clone hh = 2160;  
clone hi = 2170;  
clone hj = 2180;  
clone hk = 2190;  
clone hl = 2200;  
clone hm = 2210;  
clone hn = 2220;  
clone ho = 2230;  
clone hp = 2240;  
clone hq = 2250;  
clone hr = 2260;  
clone hs = 2270;  
clone ht = 2280;  
clone hu = 2290;  
clone hv = 2300;  
clone hw = 2310;  
clone hx = 2320;  
clone hy = 2330;  
clone hz = 2340;  
clone ia = 2350;  
clone ib = 2360;  
clone ic = 2370;  
clone id = 2380;  
clone ie = 2390;  
clone if = 2400;  
clone ig = 2410;  
clone ih = 2420;  
clone ii = 2430;  
clone ij = 2440;  
clone ik = 2450;  
clone il = 2460;  
clone im = 2470;  
clone in = 2480;  
clone io = 2490;  
clone ip = 2500;  
clone iq = 2510;  
clone ir = 2520;  
clone is = 2530;  
clone it = 2540;  
clone iu = 2550;  
clone iv = 2560;  
clone iw = 2570;  
clone ix = 2580;  
clone iy = 2590;  
clone iz = 2600;  
clone ja = 2610;  
clone jb = 2620;  
clone jc = 2630;  
clone jd = 2640;  
clone je = 2650;  
clone jf = 2660;  
clone jg = 2670;  
clone jh = 2680;  
clone ji = 2690;  
clone jj = 2700;  
clone jk = 2710;  
clone jl = 2720;  
clone jm = 2730;  
clone jn = 2740;  
clone jo = 2750;  
clone jp = 2760;  
clone jq = 2770;  
clone jr = 2780;  
clone js = 2790;  
clone jt = 2800;  
clone ju = 2810;  
clone jv = 2820;  
clone jw = 2830;  
clone jx = 2840;  
clone jy = 2850;  
clone jz = 2860;  
clone ka = 2870;  
clone kb = 2880;  
clone kc = 2890;  
clone kd = 2900;  
clone ke = 2910;  
clone kf = 2920;  
clone kg = 2930;  
clone kh = 2940;  
clone ki = 2950;  
clone kj = 2960;  
clone kk = 2970;  
clone kl = 2980;  
clone km = 2990;  
clone kn = 3000;  
clone ko = 3010;  
clone kp = 3020;  
clone kq = 3030;  
clone kr = 3040;  
clone ks = 3050;  
clone kt = 3060;  
clone ku = 3070;  
clone kv = 3080;  
clone kw = 3090;  
clone kx = 3100;  
clone ky = 3110;  
clone kz = 3120;  
clone la = 3130;  
clone lb = 3140;  
clone lc = 3150;  
clone ld = 3160;  
clone le = 3170;  
clone lf = 3180;  
clone lg = 3190;  
clone lh = 3200;  
clone li = 3210;  
clone lj = 3220;  
clone lk = 3230;  
clone ll = 3240;  
clone lm = 3250;  
clone ln = 3260;  
clone lo = 3270;  
clone lp = 3280;  
clone lq = 3290;  
clone lr = 3300;  
clone ls = 3310;  
clone lt = 3320;  
clone lu = 3330;  
clone lv = 3340;  
clone lw = 3350;  
clone lx = 3360;  
clone ly = 3370;  
clone lz = 3380;  
clone ma = 3390;  
clone mb = 3400;  
clone mc = 3410;  
clone md = 3420;  
clone me = 3430;  
clone mf = 3440;  
clone mg = 3450;  
clone mh = 3460;  
clone mi = 3470;  
clone mj = 3480;  
clone mk = 3490;  
clone ml = 3500;  
clone mn = 3510;  
clone mo = 3520;  
clone mp = 3530;  
clone mq = 3540;  
clone mr = 3550;  
clone ms = 3560;  
clone mt = 3570;  
clone mu = 3580;  
clone mv = 3590;  
clone mw = 3600;  
clone mx = 3610;  
clone my = 3620;  
clone mz = 3630;  
clone na = 3640;  
clone nb = 3650;  
clone nc = 3660;  
clone nd = 3670;  
clone ne = 3680;  
clone nf = 3690;  
clone ng = 3700;  
clone nh = 3710;  
clone ni = 3720;  
clone nj = 3730;  
clone nk = 3740;  
clone nl = 3750;  
clone nm = 3760;  
clone nn = 3770;  
clone no = 3780;  
clone np = 3790;  
clone nq = 3800;  
clone nr = 3810;  
clone ns = 3820;  
clone nt = 3830;  
clone nu = 3840;  
clone nv = 3850;  
clone nw = 3860;  
clone nx = 3870;  
clone ny = 3880;  
clone nz = 3890;  
clone oa = 3900;  
clone ob = 3910;  
clone oc = 3920;  
clone od = 3930;  
clone oe = 3940;  
clone of = 3950;  
clone og = 3960;  
clone oh = 3970;  
clone oi = 3980;  
clone oj = 3990;  
clone ok = 4000;  
clone ol = 4010;  
clone om = 4020;  
clone on = 4030;  
clone oo = 4040;  
clone op = 4050;  
clone oq = 4060;  
clone or = 4070;  
clone os = 4080;  
clone ot = 4090;  
clone ou = 4100;  
clone ov = 4110;  
clone ow = 4120;  
clone ox = 4130;  
clone oy = 4140;  
clone oz = 4150;  
clone pa = 4160;  
clone pb = 4170;  
clone pc = 4180;  
clone pd = 4190;  
clone pe = 4200;  
clone pf = 4210;  
clone pg = 4220;  
clone ph = 4230;  
clone pi = 4240;  
clone pj = 4250;  
clone pk = 4260;  
clone pl = 4270;  
clone pm = 4280;  
clone pn = 4290;  
clone po = 4300;  
clone pp = 4310;  
clone pq = 4320;  
clone pr = 4330;  
clone ps = 4340;  
clone pt = 4350;  
clone pu = 4360;  
clone pv = 4370;  
clone pw = 4380;  
clone px = 4390;  
clone py = 4400;  
clone pz = 4410;  
clone qa = 4420;  
clone qb = 4430;  
clone qc = 4440;  
clone qd = 4450;  
clone qe = 4460;  
clone qf = 4470;  
clone qg = 4480;  
clone qh = 4490;  
clone qi = 4500;  
clone qj = 4510;  
clone qk = 4520;  
clone ql = 4530;  
clone qm = 4540;  
clone qn = 4550;  
clone qo = 4560;  
clone qp = 4570;  
clone qq = 4580;  
clone qr = 4590;  
clone qs = 4600;  
clone qt = 4610;  
clone qu = 4620;  
clone qv = 4630;  
clone qw = 4640;  
clone qx = 4650;  
clone qy = 4660;  
clone qz = 4670;  
clone ra = 4680;  
clone rb = 4690;  
clone rc = 4700;  
clone rd = 4710;  
clone re = 4720;  
clone rf = 4730;  
clone rg = 4740;  
clone rh = 4750;  
clone ri = 4760;  
clone rj = 4770;  
clone rk = 4780;  
clone rl = 4790;  
clone rm = 4800;  
clone rn = 4810;  
clone ro = 4820;  
clone rp = 4830;  
clone rq = 4840;  
clone rr = 4850;  
clone rs = 4860;  
clone rt = 4870;  
clone ru = 4880;  
clone rv = 4890;  
clone rw = 4900;  
clone rx = 4910;  
clone ry = 4920;  
clone rz = 4930;  
clone sa = 4940;  
clone sb = 4950;  
clone sc = 4960;  
clone sd = 4970;  
clone se = 4980;  
clone sf = 4990;  
clone sg = 5000;  
clone sh = 5010;  
clone si = 5020;  
clone sj = 5030;  
clone sk = 5040;  
clone sl = 5050;  
clone sm = 5060;  
clone sn = 5070;  
clone so = 5080;  
clone sp = 5090;  
clone sq = 5100;  
clone sr = 5110;  
clone ss = 5120;  
clone st = 5130;  
clone su = 5140;  
clone sv = 5150;  
clone sw = 5160;  
clone sx = 5170;  
clone sy = 5180;  
clone sz = 5190;  
clone ta = 5200;  
clone tb = 5210;  
clone tc = 5220;  
clone td = 5230;  
clone te = 5240;  
clone tf = 5250;  
clone tg = 5260;  
clone th = 5270;  
clone ti = 5280;  
clone tj = 5290;  
clone tk = 5300;  
clone tl = 5310;  
clone tm = 5320;  
clone tn = 5330;  
clone to = 5340;  
clone tp = 5350;  
clone tq = 5360;  
clone tr = 5370;  
clone ts = 5380;  
clone tt = 5390;  
clone tu = 5400;  
clone tv = 5410;  
clone tw = 5420;  
clone tx = 5430;  
clone ty = 5440;  
clone tz = 5450;  
clone ua = 5460;  
clone ub = 5470;  
clone uc = 5480;  
clone ud = 5490;  
clone ue = 5500;  
clone uf = 5510;  
clone ug = 5520;  
clone uh = 5530;  
clone ui = 5540;  
clone uj = 5550;  
clone uk = 5560;  
clone ul = 5570;  
clone um = 5580;  
clone un = 5590;  
clone uo = 5600;  
clone up = 5610;  
clone uq = 5620;  
clone ur = 5630;  
clone us = 5640;  
clone ut = 5650;  
clone uu = 5660;  
clone uv = 5670;  
clone uw = 5680;  
clone ux = 5690;  
clone uy = 5700;  
clone uz = 5710;  
clone va = 5720;  
clone vb = 5730;  
clone vc = 5740;  
clone vd = 5750;  
clone ve = 5760;  
clone vf = 5770;  
clone vg = 5780;  
clone vh = 5790;  
clone vi = 5800;  
clone vj = 5810;  
clone vk = 5820;  
clone vl = 5830;  
clone vm = 5840;  
clone vn = 5850;  
clone vo = 5860;  
clone vp = 5870;  
clone vq = 5880;  
clone vr = 5890;  
clone vs = 5900;  
clone vt = 5910;  
clone vu = 5920;  
clone vv = 5930;  
clone vw = 5940;  
clone vx = 5950;  
clone vy = 5960;  
clone vz = 5970;  
clone wa = 5980;  
clone wb = 5990;  
clone wc = 6000;  
clone wd = 6010;  
clone we = 6020;  
clone wf = 6030;  
clone wg = 6040;  
clone wh = 6050;  
clone wi = 6060;  
clone wj = 6070;  
clone wk = 6080;  
clone wl = 6090;  
clone wm = 6100;  
clone wn = 6110;  
clone wo = 6120;  
clone wp = 6130;  
clone wq = 6140;  
clone wr = 6150;  
clone ws = 6160;  
clone wt = 6170;  
clone wu = 6180;  
clone wv = 6190;  
clone ww = 6200;  
clone wx = 6210;  
clone wy = 6220;  
clone wz = 6230;  
clone xa = 6240;  
clone xb = 6250;  
clone xc = 6260;  
clone xd = 6270;  
clone xe = 6280;  
clone xf = 6290;  
clone xg = 6300;  
clone xh = 6310;  
clone xi = 6320;  
clone xj = 6330;  
clone xk = 6340;  
clone xl = 6350;  
clone xm = 6360;  
clone xn = 6370;  
clone xo = 6380;  
clone xp = 6390;  
clone xq = 6400;  
clone xr = 6410;  
clone xs = 6420;  
clone xt = 6430;  
clone xu = 6440;  
clone xv = 6450;  
clone xw = 6460;  
clone xx = 6470;  
clone xy = 6480;  
clone xz = 6490;  
clone ya = 6500;  
clone yb = 6510;  
clone yc = 6520;  
clone yd = 6530;  
clone ye = 6540;  
clone yf = 6550;  
clone yg = 6560;  
clone yh = 6570;  
clone yi = 6580;  
clone yj = 6590;  
clone yk = 6600;  
clone yl = 6610;  
clone ym = 6620;  
clone yn = 6630;  
clone yo = 6640;  
clone yp = 6650;  
clone yq = 6660;  
clone yr = 6670;  
clone ys = 6680;  
clone yt = 6690;  
clone yu = 6700;  
clone yv = 6710;  
clone yw = 6720;  
clone yx = 6730;  
clone yy = 6740;  
clone yz = 6750;  
clone za = 6760;  
clone zb = 6770;  
clone zc = 6780;  
clone zd = 6790;  
clone ze = 6800;  
clone zf = 6810;  
clone zg = 6820;  
clone zh = 6830;  
clone zi = 6840;  
clone zj = 6850;  
clone zk = 6860;  
clone zl = 6870;  
clone zm = 6880;  
clone zn = 6890;  
clone zo = 6900;  
clone zp = 6910;  
clone zq = 6920;  
clone zr = 6930;  
clone zs = 6940;  
clone zt = 6950;  
clone zu = 6960;  
clone zv = 6970;  
clone zw = 6980;  
clone zx = 6990;  
clone zy = 7000;  
clone zz = 7010;  
clone aa = 7020;  
clone ab = 7030;  
clone ac = 7040;  
clone ad = 7050;  
clone ae = 7060;  
clone af = 7070;  
clone ag = 7080;  
clone ah = 7090;  
clone ai = 7100;  
clone aj = 7110;  
clone ak = 7120;  
clone al = 7130;  
clone am = 7140;  
clone an = 7150;  
clone ao = 7160;  
clone ap = 7170;  
clone aq = 7180;  
clone ar = 7190;  
clone as = 7200;  
clone at = 7210;  
clone au = 7220;  
clone av = 7230;  
clone aw = 7240;  
clone ax = 7250;  
clone ay = 7260;  
clone az = 7270;  
clone ba = 7280;  
clone bb = 7290;  
clone bc = 7300;  
clone bd = 7310;  
clone be = 7320;  
clone bf = 7330;  
clone bg = 7340;  
clone bh = 7350;  
clone bi = 7360;  
clone bj = 7370;  
clone bk = 7380;  
clone bl = 7390;  
clone bm = 7400;  
clone bn = 7410;  
clone bo = 7420;  
clone bp = 7430;  
clone bq = 7440;  
clone br = 7450;  
clone bs = 7460;  
clone bt = 7470;  
clone bu = 7480;  
clone bv = 7490;  
clone bw = 7500;  
clone bx = 7510;  
clone by = 7520;  
clone bz = 7530;  
clone ca = 7540;  
clone cb = 7550;  
clone cc = 7560;  
clone cd = 7570;  
clone ce = 7580;  
clone cf = 7590;  
clone cg = 7600;  
clone ch = 7610;  
clone ci = 7620;  
clone cj = 7630;  
clone ck = 7640;  
clone cl = 7650;  
clone cm = 7660;  
clone cn = 7670;  
clone co = 7680;  
clone cp = 7690;  
clone cq = 7700;  
clone cr = 7710;  
clone cs = 7720;  
clone ct = 7730;  
clone cu = 7740;  
clone cv = 7750;  
clone cw = 7760;  
clone cx = 7770;  
clone cy = 7780;  
clone cz = 7790;  
clone da = 7800;  
clone db = 7810;  
clone dc = 7820;  
clone dd = 7830;  
clone de = 7840;  
clone df = 7850;  
clone dg = 7860;  
clone dh = 7870;  
clone di = 7880;  
clone dj = 7890;  
clone dk = 7900;  
clone dl = 7910;  
clone dm = 7920;  
clone dn = 7930;  
clone do = 7940;  
clone dp = 7950;  
clone dq = 7960;  
clone dr = 7970;  
clone ds = 7980;  
clone dt = 7990;  
clone du = 8000;  
clone dv = 8010;  
clone dw = 8020;  
clone dx = 8030;  
clone dy = 8040;  
clone dz = 8050;  
clone ea = 8060;  
clone eb = 8070;  
clone ec = 8080;  
clone ed = 8090;  
clone ee = 8100;  
clone ef = 8110;  
clone eg = 8120;  
clone eh = 8130;  
clone ei = 8140;  
clone ej = 8150;  
clone ek = 8160;  
clone el = 8170;  
clone em = 8180;  
clone en = 8190;  
clone eo = 8200;  
clone ep = 8210;  
clone eq = 8220;  
clone er = 8230;  
clone es = 8240;  
clone et = 8250;  
clone eu = 8260;  
clone ev = 8270;  
clone ew = 8280;  
clone ex = 8290;  
clone ey = 8300;  
clone ez = 8310;  
clone fa = 8320;  
clone fb = 8330;  
clone fc = 8340;  
clone fd = 8350;  
clone fe = 8360;  
clone ff = 8370;  
clone fg = 8380;  
clone fh = 8390;  
clone fi = 8400;  
clone fj = 8410;  
clone fk = 8420;  
clone fl = 8430;  
clone fm = 8440;  
clone fn = 8450;  
clone fo = 8460;  
clone fp = 8470;  
clone fq = 8480;  
clone fr = 8490;  
clone fs = 8500;  
clone ft = 8510;  
clone fu = 8520;  
clone fv = 8530;  
clone fw = 8540;  
clone fx = 8550;  
clone fy = 8560;  
clone fz = 8570;  
clone ga = 8580;  
clone gb = 8590;  
clone gc = 8600;  
clone gd = 8610;  
clone ge = 8620;  
clone gf = 8630;  
clone gg = 8640;  
clone gh = 8650;  
clone gi = 8660;  
clone gj = 8670;  
clone gk = 8680;  
clone gl = 8690;  
clone gm = 8700;  
clone gn = 8710;  
clone go = 8720;  
clone gp = 8730;  
clone gq = 8740;  
clone gr = 8750;  
clone gs = 8760;  
clone gt = 8770;  
clone gu = 8780;  
clone gv = 8790;  
clone gw = 8800;  
clone gx = 8810;  
clone gy = 8820;  
clone gz = 8830;  
clone ha = 8840;  
clone hb = 8850;  
clone hc = 8860;  
clone hd = 8870;  
clone he = 8880;  
clone hf = 8890;  
clone hg = 8900;  
clone hh = 8910;  
clone hi = 8920;  
clone hj = 8930;  
clone hk = 8940;  
clone hl = 8950;  
clone hm = 8960;  
clone hn = 8970;  
clone ho = 8980;  
clone hp = 8990;  
clone hq = 9000;  
clone hr = 9010;  
clone hs = 9020;  
clone ht = 9030;  
clone hu = 9040;  
clone hv = 9050;  
clone hw = 9060;  
clone hx = 9070;  
clone hy = 9080;  
clone hz = 9090;  
clone ia = 9100;  
clone ib = 9110;  
clone ic = 9120;  
clone id = 9130;  
clone ie = 9140;  
clone if = 9150;  
clone ig = 9160;  
clone ih = 9170;  
clone ii = 9180;  
clone ij = 9190;  
clone ik = 9200;  
clone il = 9210;  
clone im = 9220;  
clone in = 9230;  
clone io = 9240;  
clone ip = 9250;  
clone iq = 9260;  
clone ir = 9270;  
clone is = 9280;  
clone it = 9290;  
clone iu = 9300;  
clone iv = 9310;  
clone iw = 9320;  
clone ix = 9330;  
clone iy = 9340;  
clone iz = 9350;  
clone ja = 9360;  
clone jb = 9370;  
clone jc = 9380;  
clone jd = 9390;  
clone je = 9400;  
clone jf = 9410;  
clone jg = 9420;  
clone jh = 9430;  
clone ji = 9440;  
clone jj = 9450;  
clone jk = 9460;  
clone jl = 9470;  
clone jm = 9480;  
clone jn = 9490;  
clone jo = 9500;  
clone jp = 9510;  
clone jq = 9520;  
clone jr = 9530;  
clone js = 9540;  
clone jt = 9550;  
clone ju = 9560;  
clone jv = 9570;  
clone jw = 9580;  
clone jx = 9590;  
clone jy = 9600;  
clone jz = 9610;  
clone ka = 9620;  
clone kb = 9630;  
clone kc = 9640;  
clone kd = 9650;  
clone ke = 9660;  
clone kf = 9670;  
clone kg = 9680;  
clone kh = 9690;  
clone ki = 9700;  
clone kj = 9710;  
clone kk = 9720;  
clone kl = 9730;  
clone km = 9740;  
clone kn = 9750;  
clone ko = 9760;  
clone kp = 9770;  
clone kq = 9780;  
clone kr = 9790;  
clone ks = 9800;  
clone kt = 9810;  
clone ku = 9820;  
clone kv = 9830;  
clone kw = 9840;  
clone kx = 9850;  
clone ky = 9860;  
clone kz = 9870;  
clone la = 9880;  
clone lb = 9890;  
clone lc = 9900;  
clone ld = 9910;  
clone le = 9920;  
clone lf = 9930;  
clone lg = 9940;  
clone lh = 9950;  
clone li = 9960;  
clone lj = 9970;  
clone lk = 9980;  
clone ll = 9990;  
clone lm = 10000;  
clone ln = 10010;  
clone lo = 10020;  
clone lp = 10030;  
clone lq = 10040;  
clone lr = 10050;  
clone ls = 10060;  
clone lt = 10070;  
clone lu = 10080;  
clone lv = 10090;  
clone lw = 10100;  
clone lx = 10110;  
clone ly = 10120;  
clone lz = 10130;  
clone ma = 10140;  
clone mb = 10150;  
clone mc = 10160;  
clone md = 10170;  
clone me = 10180;  
clone mf = 10190;  
clone mg = 10200;  
clone mh = 10210;  
clone mi = 10220;  
clone mj = 10230;  
clone mk = 10240;  
clone ml = 10250;  
clone mn = 10260;  
clone mo = 10270;  
clone mp = 10280;  
clone mq = 10290;  
clone mr = 10300;  
clone ms = 10310;  
clone mt = 10320;  
clone mu = 10330;  
clone mv = 10340;  
clone mw = 10350;  
clone mx = 10360;  
clone my = 10370;  
clone mz = 10380;  
clone na = 10390;  
clone nb = 10400;  
clone nc = 10410;  
clone nd = 10420;  
clone ne = 10430;  
clone nf = 10440;  
clone ng = 10450;  
clone nh = 10460;  
clone ni = 10470;  
clone nj = 10480;  
clone nk = 10490;  
clone nl = 10500;  
clone nm = 10510;  
clone nn = 10520;  
clone no = 10530;  
clone np = 10540;  
clone nq = 10550;  
clone nr = 10560;  
clone ns = 10570;  
clone nt = 10580;  
clone nu = 10590;  
clone nv = 10600;  
clone ow = 10610;  
clone ox = 10620;  
clone oy = 10630;  
clone oz = 10640;  
clone pa = 10650;  
clone pb = 10660;  
clone pc = 10670;  
clone pd = 10680;  
clone pe = 10690;  
clone pf = 10700;  
clone pg = 10710;  
clone ph = 10720;  
clone pi = 10730;  
clone pj = 10740;`

## lodash v4.15.0

A modern JavaScript utility library delivering modularity, performance, & extras.

```
_.assign({ 'a': 1 }, { 'b': 2 }, { 'c': 3 });  
// → { 'a': 1, 'b': 2, 'c': 3 }  
_.map([1, 2, 3], function(n) { return n * 3; });  
// → [3, 6, 9]
```

The background of the slide features a solid green-to-yellow gradient. Scattered across this background are several three-dimensional purple cubes of varying sizes and orientations. Some cubes are in sharp focus, while others are blurred, creating a sense of depth. The cubes are arranged in a non-uniform, abstract pattern.

**Let's take a look at some  
potential scenarios**



# Ways to cause damage

- Create a useful module
  - Use good old marketing
  - Update it after it gets adoption
- Create a module named similarly to another popular module (Typo attacks)
  - Packages are identified by names (No unique identifier/key)
- Take control of a legit account
- Create a self replicating worm

# Creating a self replicating NPM worm (Lifecycle Scripts)



- Socially engineer a npm module owner to npm install an infected module on their system.
- Worm creates a new npm module



npm install Hydra\_A

```
"scripts": {  
  "start": "node create malicious_npm_module",  
  "predeploy": "echo im about to deploy",  
  "postdeploy": "echo ive deployed",  
  "prepublish": "coffee --bare --compile --output  
lib/foo src/foo/*.coffee"
```

Full reports by Sam Saccone

[https://www.kb.cert.org/CERT\\_WEB/services/vul-notes.nsf/6eacfaeab94596f5852569290066a50b/018dbb99def6980185257f820013f175/\\$FILE/npmwormdisclosure.pdf](https://www.kb.cert.org/CERT_WEB/services/vul-notes.nsf/6eacfaeab94596f5852569290066a50b/018dbb99def6980185257f820013f175/$FILE/npmwormdisclosure.pdf)

# Creating a self replicating NPM worm (Persistent Auth)



- Worm sets lifecycle hook on the new module to execute the worm on any install
- Worm publishes the new module to the user's npm account



John

npm publish



John

Legit 1

Legit 2

**malicious\_npm\_module**

**Full reports by Sam Saccone**

[https://www.kb.cert.org/CERT\\_WEB/services/vul-notes.nsf/6eacfaeab94596f5852569290066a50b/018dbb99def6980185257f820013f175/\\$FILE/npmwormdisclosure.pdf](https://www.kb.cert.org/CERT_WEB/services/vul-notes.nsf/6eacfaeab94596f5852569290066a50b/018dbb99def6980185257f820013f175/$FILE/npmwormdisclosure.pdf)

# Creating a self replicating NPM worm (Semver)



- Worm walks all user's npm modules (publish permissions) and adds new module as a dependency in package.json.
- Worm publishes new versions to each of the modules with a "bugfix" level semver bump.



John


## Package.json

```
"dependencies": {  
  "primus": "*",  
  "async": "~0.8.0",  
  "express": "4.2.x",  
  "malicious_npm_module": "  

```

## Full reports by Sam Saccone

[https://www.kb.cert.org/CERT\\_WEB/services/vul-notes.nsf/6eacfaeab94596f5852569290066a50b/018dbb99def6980185257f820013f175/\\$FILE/npmwormdisclosure.pdf](https://www.kb.cert.org/CERT_WEB/services/vul-notes.nsf/6eacfaeab94596f5852569290066a50b/018dbb99def6980185257f820013f175/$FILE/npmwormdisclosure.pdf)

The background of the slide features a solid green-to-yellow gradient. Scattered across this background are several three-dimensional purple cubes of varying sizes and orientations. Some cubes are in sharp focus, while others are blurred, creating a sense of depth. The cubes are arranged in a way that suggests a random or careless placement.

Less Malicious –  
more Careless –  
still Vulnerable

## What is wrong with this picture?

```
return function middleware (req, res, next) {  
  // Strip any null bytes from the url  
  while(req.url.indexOf('%00') !== -1) {  
    req.url = req.url.replace(/\\%00/g, '');  
  }  
}
```










# What we did

- Scan for security issues
  - Top 50 popular packages
  - Top 50 dependent-upon packages
  - Other popular packages
- Analyze results
- Responsible Disclosure
  - Contact dev
  - Wait for patch
  - Publish



# Top 50 NPM packages

## Packages people 'npm install' a lot

 <b>browserify</b> browser-side require() the nod... 13.0.1 published 4 months ago by jmm	 <b>gulp</b> The streaming build system 3.9.1 published 7 months ago by phated	 <b>npm</b> a package manager for JavaSc... 3.9.0 published 3 months ago by zkat
 <b>grunt-cli</b> The grunt command line interf... 1.2.0 published 5 months ago by vladikoff	 <b>grunt</b> The JavaScript Task Runner 1.0.1 published 5 months ago by shame	 <b>cordova</b> Cordova command line interfa... 6.2.0 published 4 months ago by stevegill
 <b>bower</b> The browser package manager 1.7.9 published 5 months ago by shreen	 <b>express</b> Fast, unopinionated, minimal... 4.14.0 published 3 months ago by rimasthurs	 <b>forever</b> A simple CLI tool for ensuring ... 0.15.2 published 4 months ago by indexzero

<https://www.npmjs.com/>

## Most depended-upon packages

 <b>lodash</b> Lodash modular utilities. 4.15.0 published 4 weeks ago by dalton	 <b>underscore</b> JavaScript's functional programming help... 1.8.3 published a year ago by jashkenas	 <b>bluebird</b> Full featured Promises/A+ implementatio... 3.4.6 published a week ago by esajje
 <b>request</b> Simplified HTTP request client. 2.74.0 published 2 months ago by simov	 <b>express</b> Fast, unopinionated, minimalist web fra... 4.14.0 published 3 months ago by dougwtson	 <b>chalk</b> Terminal string styling done right. Much ... 1.1.3 published 5 months ago by qix
 <b>async</b> Higher-order functions and common patt... 2.0.1 published 2 months ago by megawac	 <b>commander</b> the complete solution for node.js comm... 2.9.0 published 11 months ago by zhyeleee	 <b>debug</b> small debugging utility 2.2.0 published a year ago by tootallnate

<https://www.npmjs.com/>



## Scan for security issues



PROJECT NAME	LAST SCAN DATE	TEAM	LOC
<u>acorn-master</u>	6/22/2016	CxServer\SP\Company\npm project	97564
<u>ansi-regex-master</u>	6/22/2016	CxServer\SP\Company\npm project	414
<u>esprima-master</u>	6/22/2016	CxServer\SP\Company\npm project	75907
<u>inherits-master</u>	6/23/2016	CxServer\SP\Company\npm project	47
<u>isarray-master</u>	6/23/2016	CxServer\SP\Company\npm project	25
<u>lodash-master</u>	6/23/2016	CxServer\SP\Company\npm project	128337
<u>object-keys-master</u>	6/23/2016	CxServer\SP\Company\npm project	419
<u>private-master</u>	6/23/2016	CxServer\SP\Company\npm project	198

⏪

⏩

1

⏪

⏩

Page size: 

All

# What is wrong with this picture?

```
46
47
48 return function middleware (req, res, next) {
49
50     // Strip any null bytes from the url
51     while(req.url.indexOf('%00') !== -1) {
52         req.url = req.url.replace(/%00/g, '');
53     }
54     // Figure out the path for the file from the given url
55     var parsed = url.parse(req.url);
56     try {
57         decodeURIComponent(req.url); // check validity of url
58         var pathname = decodeURIComponent(parsed.pathname);
59     }
60     catch (err) {
61         return status[400](res, next, { error: err });
62     }
63
64     var file = path.normalize(
65         path.join(root,
66             path.relative(
67                 path.join('/', baseDir),
68                 pathname
```

Scan Results

Severity

JavaScript

- High
  - Reflected\_XSS (2 : Found) (?)
- Medium
  - Server\_DoS\_by\_loop (2 : Found) (?)

Results

Graph

Result State	Result Severity	Assign to User	Comments	Save Scan Subset	Open Ticket				
Id	Dir	Status	Source Folder	Source Filename	Source Line	Source Object	Destination Folder	Destination File	Des
1		New	\node-ecs...	ecstatic.js	51	indexOf	\node-ecs...	ecstatic.js	51
2		New	\node-ecs...	ecstatic.js	52	replace	\node-ecs...	ecstatic.js	51

# What is wrong with this picture?

## ecstatic

```
return function middleware (req, res, next) {  
  // Strip any null bytes from the url  
  while(req.url.indexOf('%00') !== -1) {  
    req.url = req.url.replace(/\\%00/g, '');  
  }  
}
```

- 150k weekly downloads
- **263** other npm packages are dependent on ecstatic

## Developer Response

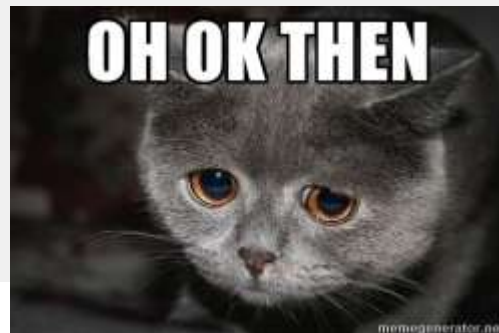


### ■ PoC:

- 22kb payload - 1 sec lag
- 35kb payload - 3 sec lag
- 86kb payload - **server crashed**

} <http://www.checkmarx.com/%00%00%00%00%00%00> (...)

# Developer Response



```
return function middleware (req, res, next) {  
  // Strip any null bytes from the url  
  // This was at one point necessary because of an old bug in url.parse  
  //  
  // See: https://github.com/jfhbrook/node-ecstatic/issues/16#issuecomment-3039914  
  // See: https://github.com/jfhbrook/node-ecstatic/commit/43f7e72a31524f88f47e367c3cc3af710e67c9f4  
  //  
  // But this opens up a regex dos attack vector! D:  
  //  
  // Based on some research (ie asking #node-dev if this is still an issue),  
  // it's *probably* not an issue. :)  
  /*  
  while(req.url.indexOf('%00') !== -1) {  
    req.url = req.url.replace(/\\%00/g, '');  
  }  
  */  
}
```

- **Command Injection**

- Variable from user input was used as an argument for an OS command.
- Dev response: “The flaw exists because the original author used it... A possible solution is to delete the vulnerable file”.

## Other Scan Results

- **Command Injection**
- **Stored XSS**
- **Denial of Service by Loop**
- **Denial of Service by Regex (ReDoS)**
- **CSV Injection**
- **Insecure Randomness**
- **Open Redirect**

The background features a solid green-to-yellow gradient. On the left side, there is a cluster of several 3D purple cubes of varying sizes, some stacked and some floating. A few more cubes are scattered in the lower foreground. On the right side, there is a blurred, out-of-focus purple cube.

So how do I protect  
myself?



# Be a Safe User!

- Check if there are any hooks: **npm show \$module scripts**
- Inspect module's code - and check out its dependencies
- Don't allow scripts to execute automatically: **npm install --ignorescripts**
- Use **npm shrinkwrap** to lock down your own dependencies
- Sometimes it's better to write your own functions!
- Analyze your own code *together* with its dependencies!
- Enable 2FA and/or log out!



# Be a Safe Corporate User!

- Run a local NPM Registry
- Replicate official registry ... or not
- Prevent installing from main registry



The background of the slide is decorated with several 3D purple cubes of varying sizes and orientations. Some cubes are clustered together on the left and bottom right, while others are isolated, such as one in the upper right and another in the lower left. The cubes have a matte finish and cast soft shadows.

**Thank You.**