

UNICOS LOCAL HOLE ALL VERSIONS

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2001-11/0227.html>

From: Mickey Mouse (mmsquadron@hotmail.com)

Date: 11/27/01

From: "Mickey Mouse" <mmsquadron@hotmail.com>
To: bugtraq@securityfocus.com
Subject: UNICOS LOCAL HOLE ALL VERSIONS
Date: Tue, 27 Nov 2001 22:06:21 +0000
Message-ID: <F27191E9GQvnbEG10Ga00026dbd@hotmail.com>

***** CRAY UNICOS NQSD FORMAT BUG LOCAL ROOT COMPROMISE ALL VERSIONS

MICKEY MOUSE HACKING SQUADRON ADVISORY #: 1

DISCLAIMER

We are a collective group of security professionals who want to remain nameless due to the various legal and corporate red tape which now surrounds the issue of disclosure in today's IT security environments. However, due to the fact that we have unsuccessfully been able to convince vendors to take appropriate actions in fixing these gaping security holes, we have decided to take the option of becoming nameless and releasing this advisory in such a way. Due to the nature of many of the severe vulnerabilities we have discovered, we will enclose only minimal details about the holes, and no working exploit code.

BEGIN

NATURE

Local root compromise of any UNICOS computer running the NQS daemon

VULNERABLE PLATFORMS/SOFTWARE

All versions of cray's UNIX Cray Operating System running NQSD
Possibly NQSD running in IBM and Solaris environments as well.

SUCCESSFULLY TESTED ON

Cray T3E running UNICOS/mk revision 2.0.5.54

UNICOS LOCAL HOLE ALL VERSIONS

SecurityFocus Bugtraq: UNICOS LOCAL HOLE ALL VERSIONS

HISTORY

The NQS, or Network Queueing System, is a popular batch software processor which is used to perform job control and leveraging in supercomputing environments which require heavy symmetric multi processing. The controlling daemon, which looks like it appears below

```
37152 ? 0:00 nqsdaemon
57415 ? 0:00 nqsdaemon
```

runs as root in order to properly schedule and timeslice batched process. The Mickey Mouse Hacking Squadron has discovered a format bug vulnerability by which any unprivileged user on a system running NQS can gain root access. This involves creating a batch with a name that contains special formatting characters, which is processed by an unsafe function taking a variable argument list. In order to exploit this vulnerability, the user must be able to submit the job with qsub in such a way that it triggers this vulnerability.

DESCRIPTION

The qsub command submits a file that contains a shell script as a batch request to the Network Queueing System (NQS). For an introduction to the use of NQS, see the Network Queueing System (NQS)User's Guide, publication SG-2105.

This vulnerability has been exploited successfully by the MMHS in a RISC environment, using ALPHA processors, in a way similar to bugs exploited successfully on Digital UNIX by SeungHyun Seo, also posted to the Bugtraq mailing list. The exploitation on vectorized processors, such as the Y-MP series, has proved to be much more difficult, especially due to large 64 bit addressing and a large number of NULL bytes in the process address space. This should also prove easy to exploit on PowerPC and SPARC environments.

VENDOR STATUS

NO RESPONSE FROM CRAY!

REFERENCES

- 1). "Format String Attack on alpha system" Seunghyun Seo (truefinder), 2001/09/24
<http://cert.uni-stuttgart.de/archive/bugtraq/2001/09/msg00264.html>

CONTACT

We are looking for feedback and new members! EMAIL us with any concerns you might have.

Note: We are not a blackhat organization, just a group of concerned professionals!

SecurityFocus Bugtraq: UNICOS LOCAL HOLE ALL VERSIONS

MMSquadron@hotmail.com for any comments or suggestions!

GREETINGS

Team TESO, Aleph1, M. Zalewski, Georgi, zen-parse, Simple Nomad, HERT,
GOBBLES

Get your FREE download of MSN Explorer at <http://explorer.msn.com/intl.asp>

- *Previous message:* [Linux Mandrake Security Team: "MDKSA-2001:077-1 - apache update"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)