

RE: Bad protocol version identification '^V^C^A'

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2002-12/0002.html>

From: Bojan Zdrnja (Bojan.Zdrnja@FER.hr)

Date: 12/01/02

From: "Bojan Zdrnja" <Bojan.Zdrnja@FER.hr>
To: "'jm'" <security@wirerats.org>, <incidents@securityfocus.com>
Date: Sun, 1 Dec 2002 10:15:49 +0100

Hi.

I suppose this is plain SSHD buffer overflow attack, followed by 'id' commands. Attacker tried buffer overflow (which didn't succeed, according to logs) and after that he tried to execute 'id' commands to see if his attack worked (ie. If he managed to elevate his privileges). IIRC, SSH expects protocol identification as first data on the channel – attacker tried overflow and then 2 commands which SSHD interpreted as bad protocol identification.

I'd check sshd versions for sure, but I think this was just an attack attempt on your server.

Best regards,

Bojan Zdrnja

> -----Original Message-----
> From: jm [<mailto:security@wirerats.org>]
> Sent: 30. studeni 2002 1:25
> To: incidents@securityfocus.com
> Subject: Re: Bad protocol version identification '^V^C^A'
>
>
> In-Reply-To:
> <1395.136.159.104.19.1038501745.squirrel@webmail.enel.ucalgary.ca>
>
> I wouldn't worry too much about this. These type of log events are
> usually symbolic of some type of network scanner or brute
> force scanner.
> You can duplicate a similar log event by using nc or telnet
> and connecting
> to a 'ssh' server (nc -vv hostAddress 22). However, I would be
> concerned with whatever service you have listening that are
> identified in
> you logs before the ip address of the remote connection (ie /bin/id

SecurityFocus Incidents: RE: Bad protocol version identification '^V^C^A'

> and /usr/bin/id ...). I would check to see what these
> services are and if
> you don't need them I would disable them as it may be possible that
> someone is trying to exploit that service.
>
> jm
>
>
> >Received: (qmail 1361 invoked from network); 29 Nov 2002
> 23:47:17 -0000
> >Received: from outgoing3.securityfocus.com (205.206.231.27)
> > by mail.securityfocus.com with SMTP; 29 Nov 2002 23:47:17 -0000
> >Received: from lists.securityfocus.com (lists.securityfocus.com
> [205.206.231.19])
> > by outgoing3.securityfocus.com (Postfix) with QMQP
> > id 6F4ECA30F8; Fri, 29 Nov 2002 16:38:26 -0700 (MST)
> >Mailing-List: contact incidents-help@securityfocus.com; run by ezmlm
> >Precedence: bulk
> >List-Id: <incidents.list-id@securityfocus.com>
> >List-Post: <<mailto:incidents@securityfocus.com>>
> >List-Help: <<mailto:incidents-help@securityfocus.com>>
> >List-Unsubscribe: <<mailto:incidents-unsubscribe@securityfocus.com>>
> >List-Subscribe: <<mailto:incidents-subscribe@securityfocus.com>>
> >Delivered-To: mailing list incidents@securityfocus.com
> >Delivered-To: moderator for incidents@securityfocus.com
> >Received: (qmail 9369 invoked from network); 28 Nov 2002
> 16:22:05 -0000
> >From: Randy Millis <rmillisl@enel.ucalgary.ca>
> >Message-ID:
> ><1395.136.159.104.19.1038501745.squirrel@webmail.enel.ucalgary.ca>
> >Date: Thu, 28 Nov 2002 09:42:25 -0700 (MST)
> >Subject: Bad protocol version identification '^V^C^A'
> >To: <incidents@securityfocus.com>
> >X-Priority: 3
> >Importance: Normal
> >X-Mailer: SquirrelMail (version 1.2.8)
> >MIME-Version: 1.0
> >Content-Type: text/plain; charset=iso-8859-1
> >Content-Transfer-Encoding: 8bit
> >
> >Had the following entries in brought to my attention by
> >LogWatch this
> >morning.
> >
> >Can anyone guide me to what they might be and if I need to
> >be concerned
> >about them?
> >
> >Thanks.
> >
> >----- SSHD Begin -----

RE: Bad protocol version identification '^V^C^A'

SecurityFocus Incidents: RE: Bad protocol version identification '^V^C^A'

```
> >
> > **Unmatched Entries**
> > Bad protocol version identification '^V^C^A' from
> xxx.xxx.xxx.xxx Bad
> > protocol version identification '^V^C' from xxx.xxx.xxx.xxx Bad
> > protocol version identification '^' from xxx.xxx.xxx.xxx Bad
> protocol
> > version identification '^/bin/id` #' from xxx.xxx.xxx.xxx
> Bad protocol
> > version identification '^/usr/bin/id` #' from xxx.xxx.xxx.xxx
> >
> >
> > ----- SSHD End -----
> >
> >
> > -----
> -----
> > ---
> --
> > This list is provided by the SecurityFocus ARIS analyzer
> service. For
> > more information on this free incident handling, management and
> > tracking system please see: http://aris.securityfocus.com
> >
> >
> >
> -----
> -----
> This list is provided by the SecurityFocus ARIS analyzer
> service. For more information on this free incident handling,
> management
> and tracking system please see: http://aris.securityfocus.com
>
>
```

This list is provided by the SecurityFocus ARIS analyzer service.
For more information on this free incident handling, management
and tracking system please see: <http://aris.securityfocus.com>